日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２０００年　５月３０日

出願番号
Application Number: 特願２０００－１６０００１

出願人
Applicant (s): 株式会社日立製作所

CERTIFIED COPY OF
PRIORITY DOCUMENT

２００１年　３月　２日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号　出証特２００１－３０１５４０３

【書類名】　特許願
【整理番号】　H0000508
【あて先】　特許庁長官殿
【国際特許分類】　G09C　1/00
【発明者】
　【住所又は居所】　神奈川県横浜市戸塚区戸塚町５０３０番地　株式会社日立製作所　ソフトウェア事業部内
　【氏名】　桶屋　勝幸
【特許出願人】
　【識別番号】　000005108
　【氏名又は名称】　株式会社日立製作所
【代理人】
　【識別番号】　100096954
　【弁理士】
　【氏名又は名称】　矢島　保夫
【手数料の表示】
　【予納台帳番号】　022781
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　楕円曲線暗号におけるスカラー倍計算方法及び装置、並びに記憶媒体

【特許請求の範囲】

【請求項１】

楕円曲線暗号においてスカラー値及び楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、

前記スカラー値のビットの値を判定するステップと、前記判定を行なったビットの値に依存せずに一定の回数及び一定の順序で楕円曲線上の演算を実行するステップとを含むことを特徴とするスカラー倍計算方法。

【請求項２】

楕円曲線暗号においてスカラー値及び楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、

前記スカラー値のビットの値を判定するステップと、楕円曲線上の加算及び楕円曲線上の２倍算を、楕円曲線上の加算を実行した後、楕円曲線上の２倍算を実行するという順序で行なうステップとを含むことを特徴とするスカラー倍計算方法。

【請求項３】

楕円曲線暗号においてスカラー値及び楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、

前記スカラー値のビットの値を判定するステップと、楕円曲線上の加算及び楕円曲線上の２倍算を、楕円曲線上の２倍算を実行した後、楕円曲線上の加算を実行するという順序で行なうステップとを含むことを特徴とするスカラー倍計算方法。

【請求項４】

楕円曲線暗号においてスカラー値及び楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、

前記スカラー値のビットの値を判定するステップと、楕円曲線上の加算及び楕円曲線上の２倍算を同時に実行するステップとを含むことを特徴とするスカラー

倍計算方法。

【請求項５】

楕円曲線暗号においてスカラー値及び楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、

楕円曲線上の加算を実行するステップと、前記スカラー値のビットの値を判定するステップと、楕円曲線上の２倍算を実行するステップとを含むことを特徴とするスカラー倍計算方法。

【請求項６】

楕円曲線暗号においてスカラー値及び楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、

楕円曲線上の加算及び楕円曲線上の２倍算の計算順序をランダム化するステップと、前記スカラー値のビットの値を判定するステップと、楕円曲線上の加算及び楕円曲線上の２倍算を、前記加算及び２倍算の計算順序をランダム化するステップによりランダム化された順序で行なうステップとを含むことを特徴とするスカラー倍計算方法。

【請求項７】

楕円曲線暗号においてスカラー値及び楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、

前記スカラー値のビットの値を判定するステップと、楕円曲線上の加算及び楕円曲線上の２倍算の計算順序をランダム化するステップと、楕円曲線上の加算及び楕円曲線上の２倍算を、前記加算及び２倍算の計算順序をランダム化するステップによりランダム化された順序で行なうステップとを含むことを特徴とするスカラー倍計算方法。

【請求項８】

第１のデータから第２のデータを生成するデータ生成方法であって、請求項１から７の何れか１つに記載のスカラー倍計算方法を用いてスカラー倍を計算するステップを有することを特徴とするデータ生成方法。

【請求項９】

データから署名データを生成する署名生成方法であって、請求項１から７の何

れか１つに記載のスカラー倍計算方法を用いてスカラー倍を計算するステップを有することを特徴とする署名生成方法。

【請求項１０】

暗号化されたデータから復号化されたデータを生成する復号化方法であって、請求項１から７の何れか１つに記載のスカラー倍計算方法を用いてスカラー倍を計算するステップを有することを特徴とする復号化方法。

【請求項１１】

楕円曲線暗号においてスカラー値及び楕円曲線上の点からスカラー倍点を計算するスカラー倍計算装置であって、

前記スカラー値のビットの値を判定するビット値判定手段と、楕円曲線上の加算を実行する加算演算手段と、楕円曲線上の２倍算を実行する２倍算演算手段とを具備し、

前記ビット値判定手段により前記スカラー値のビットの値を判定した後、前記加算演算手段及び２倍算演算手段により楕円曲線上の加算及び楕円曲線上の２倍算を一定の回数及び一定の順序で実行し、スカラー倍点を計算することを特徴とするスカラー倍計算装置。

【請求項１２】

請求項１から７の何れか１つに記載のスカラー倍計算方法に係るプログラムを格納したことを特徴とする記憶媒体。

【請求項１３】

請求項１から７の何れか１つに記載のスカラー倍計算方法において、前記楕円曲線としてモンゴメリ型楕円曲線を用いることを特徴とするスカラー倍計算方法。

【請求項１４】

請求項１から７の何れか１つに記載のスカラー倍計算方法において、前記楕円曲線として標数２の有限体上で定義された楕円曲線を用いることを特徴とするスカラー倍計算方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、コンピュータネットワークにおけるセキュリティ技術に関し、特に楕円曲線暗号における暗号処理方法及び装置並びに記憶媒体に関する。

【０００２】

【従来の技術】

楕円曲線暗号は、N.Koblitz，V.S.Millerにより提案された公開鍵暗号の一種である。公開鍵暗号には、公開鍵と呼ばれる一般に公開してよい情報と、秘密鍵と呼ばれる秘匿しなければならない秘密情報がある。与えられたメッセージの暗号化や署名の検証には公開鍵を用い、与えられたメッセージの復号化や署名の作成には秘密鍵を用いる。楕円曲線暗号における秘密鍵は、スカラー値が担っている。また、楕円曲線暗号の安全性は、楕円曲線上の離散対数問題の求解が困難であることに由来している。ここで楕円曲線上の離散対数問題とは、楕円曲線上のある点Ｐとそのスカラー倍の点ｄＰが与えられたとき、スカラー値ｄを求める問題である。ここにおいて、楕円曲線上の点とは、楕円曲線の定義方程式をみたす数の組をいう。楕円曲線上の点全体には、無限遠点という仮想的な点を単位元とした演算、すなわち楕円曲線上の加法が定義されている。そして、同じ点同士の楕円曲線上の加法のことを、特に楕円曲線上の２倍算という。ある点に対し、特定の回数だけ加法を行なうことをスカラー倍といい、その結果をスカラー倍点、その回数のことをスカラー値という。

【０００３】

楕円曲線上の離散対数問題の求解の困難性が理論的に確立されてきている一方で、実際の実装においては秘密鍵等の秘密情報に関連する情報が暗号処理において漏洩する場合があり、その漏洩情報をもとに秘密情報を復元するといった、所謂パワーアナリシスという攻撃法が提案されている。

【０００４】

DES(Data Encryption Standard)等の秘密情報を用いた暗号処理において、電圧変化を測定することで暗号処理経過を入手し、それをもとにして秘密情報を推察するという攻撃法が、P.Kocher，J.Jaffe，B.Jun Differential Power Analysis，Advances in Cryptology: Proceedings of CRYPTO '99，LNCS 1666，Spring

er-Verlag, (1999) pp.388-397. に記載されている。この攻撃法は、DPA(Differential Power Analysis)と呼ばれている。

【０００５】

楕円曲線暗号に対して上述の攻撃法を適用したものが、J.Coron, Resistance against Differential Power Analysis for Elliptic Curve Cryptosystems, Cryptographic Hardware and Embedded Systems: Proceedings of CHES'99, LNCS 1717, Springer-Verlag, (1999) pp.292-302. に記載されている。楕円曲線暗号において、与えられたメッセージの暗号化や復号化、乃至は署名の作成及びその検証は、楕円曲線演算を用いて行なう必要がある。特に、楕円曲線上のスカラー倍の計算は、秘密情報であるスカラー値を用いた暗号処理において用いられる。

【０００６】

また、モンゴメリ型楕円曲線$BY^2=X^3+AX^2+X$（A，B∈Fp）を用いると標準型楕円曲線と呼ばれる通常用いる楕円曲線よりも高速に演算を実行できることが、P.L.Montgomery, Speeding the Pollard and Elliptic Curve Methods of Factorization, Math. Comp. 48 (1987) pp.243-264. に記載されている。これは、スカラー値の特定のビットの値に依存して、楕円曲線上の点の組（mP，（m＋１）P）から点の組（２mP，（２m＋１）P）乃至は点の組（（２m＋１）P，（２m＋２）P）を繰り返し計算するスカラー倍計算方法において、モンゴメリ型楕円曲線を利用することにより、加算及び２倍算の計算時間が短縮されることに由来する。

【０００７】

また、標数２の有限体上で定義された楕円曲線に対しても、モンゴメリ型楕円曲線におけるスカラー倍計算方法を適応させたスカラー倍計算方法並びにそれに用いる加算方法及び２倍算方法が、J.Lopez, R.Dahab, Fast Multiplication on Elliptic Curves over GF(2m) without Precomputation, Cryptographic Hardware and Embedded Systems: Proceedings of CHES'99, LNCS 1717, Springer-Verlag, (1999) pp.316-327. に記載されている。このスカラー倍計算方法における加算及び２倍算の計算時間が短縮されることにより、標数２の有限体上で定義された楕円曲線における通常のスカラー倍計算方法と比べて、スカラー倍計算が

高速に実行できる。

【０００８】

楕円曲線暗号に対するDPA攻撃の対処法の一つとして、ランダム化射影座標を用いる方法が、J.Coron, Resistance against Differential Power Analysis for Elliptic Curve Cryptosystems, Cryptographic Hardware and Embedded Systems: Proceedings of CHES'99, LNCS 1717, Springer-Verlag, (1999) pp.292-302. に記載されている。これはスカラー倍計算において、特定の値が出現するか否かを観測し、そこからスカラー値を割り出す攻撃法に対して、ランダムな値を乗ずることにより、特定の値が出現することを予測できなくする対処法である。

【０００９】

【発明が解決しようとする課題】

上記従来技術の楕円曲線暗号は、DPA等のパワーアナリシスによる攻撃については考慮されていなかった。それゆえに、パワーアナリシスによる攻撃を和らげるためには、秘密情報を用いた暗号処理において、必要な計算以外に余分な計算を行なうなどして、暗号処理経過と秘密情報との依存関係を弱くしなければならなかった。そのため、暗号処理に必要な時間が増大し、ICカード等の計算速度の遅いコンピュータや、膨大な数の暗号処理をこなすサーバ等においては、暗号処理効率の低下が目立つ状態にあった。そのうえ、暗号処理経過と秘密情報との依存関係を完全に断ち切ることはできなかった。また、暗号処理効率を優先しようとすれば、パワーアナリシスによる攻撃を受け易く、秘密情報が漏洩する可能性があるという状態にあった。

【００１０】

本発明の目的は、パワーアナリシス等により暗号処理経過が漏洩しても、秘密情報自体は漏洩せず、しかも高速に暗号処理を実行できる暗号処理方法及び装置並びに記憶媒体を提供すること、特に、秘密情報であるスカラー値から楕円曲線上のスカラー倍点を計算する計算経過からスカラー値の情報を引き出すことができないスカラー倍計算方法を提供することにある。

【００１１】

【課題を解決するための手段】

上記目的を達成するため、本発明は、楕円曲線暗号においてスカラー値及び楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、前記スカラー値のビットの値を判定するステップと、前記判定を行なったビットの値に依存せずに一定の回数及び一定の順序で楕円曲線上の演算を実行するステップとを含むことを特徴とする。

【００１２】

また本発明は、楕円曲線暗号においてスカラー値及び楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、前記スカラー値のビットの値を判定するステップと、楕円曲線上の加算及び楕円曲線上の２倍算を、楕円曲線上の加算を実行した後、楕円曲線上の２倍算を実行するという順序で行なうステップとを含むことを特徴とする。

【００１３】

また本発明は、楕円曲線暗号においてスカラー値及び楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、前記スカラー値のビットの値を判定するステップと、楕円曲線上の加算及び楕円曲線上の２倍算を、楕円曲線上の２倍算を実行した後、楕円曲線上の加算を実行するという順序で行なうステップとを含むことを特徴とする。

【００１４】

また本発明は、楕円曲線暗号においてスカラー値及び楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、前記スカラー値のビットの値を判定するステップと、楕円曲線上の加算及び楕円曲線上の２倍算を同時に実行するステップとを含むことを特徴とする。

【００１５】

また本発明は、楕円曲線暗号においてスカラー値及び楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、楕円曲線上の加算を実行するステップと、前記スカラー値のビットの値を判定するステップと、楕円曲線上の２倍算を実行するステップとを含むことを特徴とする。

【００１６】

また本発明は、楕円曲線暗号においてスカラー値及び楕円曲線上の点からスカ

ラー倍点を計算するスカラー倍計算方法であって、楕円曲線上の加算及び楕円曲線上の２倍算の計算順序をランダム化するステップと、前記スカラー値のビットの値を判定するステップと、楕円曲線上の加算及び楕円曲線上の２倍算を、前記加算及び２倍算の計算順序をランダム化するステップによりランダム化された順序で行なうステップとを含むことを特徴とする。

【００１７】

また本発明は、楕円曲線暗号においてスカラー値及び楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、前記スカラー値のビットの値を判定するステップと、楕円曲線上の加算及び楕円曲線上の２倍算の計算順序をランダム化するステップと、楕円曲線上の加算及び楕円曲線上の２倍算を、前記加算及び２倍算の計算順序をランダム化するステップによりランダム化された順序で行なうステップとを含むことを特徴とする。

【００１８】

また本発明は、第１のデータから第２のデータを生成するデータ生成方法であって、上述のスカラー倍計算方法を用いてスカラー倍を計算するステップを有することを特徴とする。さらに、データから署名データを生成する署名生成方法であって、上述のスカラー倍計算方法を用いてスカラー倍を計算するステップを有することを特徴とする。さらに、暗号化されたデータから復号化されたデータを生成する復号化方法であって、上述のスカラー倍計算方法を用いてスカラー倍を計算するステップを有することを特徴とする。

【００１９】

さらに、本発明は、楕円曲線暗号においてスカラー値及び楕円曲線上の点からスカラー倍点を計算するスカラー倍計算装置であって、前記スカラー値のビットの値を判定するビット値判定手段と、楕円曲線上の加算を実行する加算演算手段と、楕円曲線上の２倍算を実行する２倍算演算手段とを具備し、前記ビット値判定手段により前記スカラー値のビットの値を判定した後、前記加算演算手段及び２倍算演算手段により楕円曲線上の加算及び楕円曲線上の２倍算を一定の回数及び一定の順序で実行し、スカラー倍点を計算することを特徴とする。

【００２０】

さらに、本発明は、上述のスカラー倍計算方法に係るプログラムを格納したことを特徴とする記憶媒体にある。前記楕円曲線としてモンゴメリ型楕円曲線を用いるとよい。前記楕円曲線として標数２の有限体上で定義された楕円曲線を用いるとよい。

【００２１】

【発明の実施の形態】

以下、本発明の実施の形態を図面を用いて説明する。

【００２２】

図１１は、本発明の実施の形態に係る暗号処理システムの構成図である。この暗号処理システム１１０１は、例えばＩＣカード内に設けられ、暗号化（あるいは、復号化、署名の作成や検証）の際に、あるメッセージ（値）１１０５を入力すると所定の計算を行なってあるメッセージ（値）１１０６を出力する処理を行なう。暗号処理システム１１０１は、暗号処理部１１０２、スカラー倍計算部１１０３、及び秘密情報格納部１１０４を備えている。特に、本実施形態のスカラー倍計算部１１０３は、スカラー倍計算経過が漏洩しても秘密情報は漏洩しないものであり、これにより暗号処理システム１１０１は、暗号処理経過が漏洩しても秘密情報は漏洩しないシステムになっている。

【００２３】

図１６は、図１１の暗号処理システムにおける処理の流れを示すフローチャートである。図１７は、図１１の暗号処理システムにおける処理の流れを示すシーケンス図である。

【００２４】

図１６において、暗号処理システム１１０１は、以下のようにして、与えられたメッセージ１１０５から暗号処理を行なったメッセージ１１０６を出力する。まず、メッセージ１１０５を暗号処理システム１１０１に入力すると、暗号処理部１１０２がそれを受け取る（ステップ１６０１）。暗号処理部１１０２は、スカラー倍計算部１１０３に、入力メッセージ１１０５に応じた楕円曲線上の点を与える（ステップ１６０２）。スカラー倍計算部１１０３は、秘密情報格納部１１０４より秘密情報であるスカラー値を受け取る（ステップ１６０３）。スカラ

一倍計算部１１０３は、受け取った点とスカラー値より、スカラー倍点を、スカラー倍計算経過が漏洩しても秘密情報は漏洩しないスカラー倍計算方法で計算する（ステップ１６０４）。スカラー倍計算部１１０３は、計算したスカラー倍点を暗号処理部１１０２に送る（ステップ１６０５）。暗号処理部１１０２は、スカラー倍計算部１１０３より受け取ったスカラー倍点をもとにして暗号処理を行なう（ステップ１６０６）。その結果を暗号処理を行なったメッセージ１１０６として出力する（ステップ１６０７）。

【００２５】

上記処理手順を図１７のシーケンス図を用いて説明する。まず、暗号処理部１７０１（図１１の１１０２）の実行する処理について説明する。暗号処理部１７０１は、入力メッセージを受け取る。暗号処理部１７０１は、入力メッセージをもとに楕円曲線上の点を選び、スカラー倍計算部１７０２に楕円曲線上の点を与え、そしてスカラー倍計算部１７０２からスカラー倍点を受け取る。暗号処理部１７０１は、受け取ったスカラー倍点を用いて暗号処理を行ない、その結果を出力メッセージとして出力する。

【００２６】

次にスカラー倍計算部１７０２（図１１の１１０３）の実行する処理について説明する。スカラー倍計算部１７０２は、暗号処理部１７０１より楕円曲線上の点を受け取る。スカラー倍計算部１７０２は、秘密情報格納部１７０３よりスカラー値を受け取る。スカラー倍計算部１７０２は、受け取った楕円曲線上の点及びスカラー値から、スカラー倍計算経過が漏洩しても秘密情報は漏洩しないスカラー倍計算方法により、スカラー倍点を計算し、暗号処理部１７０１にスカラー倍点を送る。

【００２７】

最後に秘密情報格納部１７０３（図１１の１１０４）の実行する処理について説明する。秘密情報格納部１７０３は、スカラー倍計算部１７０２がスカラー倍を計算できるように、スカラー値をスカラー倍計算部１７０２に送る。

【００２８】

スカラー倍計算部１１０３が実行するスカラー倍計算は、スカラー倍計算経過

が漏洩しても秘密情報であるスカラー値に関する情報は漏洩しないものである。そのため、暗号処理部１１０２において、暗号処理を行なう際に暗号処理経過が漏洩したとしても、秘密情報であるスカラー値を扱っているのはスカラー倍計算部１１０３のみであり、秘密情報に関する情報は漏洩しない。

【００２９】

次に、暗号処理システム１１０１におけるスカラー倍計算部１１０３の具体的な実施例を説明する。

【００３０】

図２は、暗号処理システム１１０１における秘密情報を用いた暗号処理において、暗号処理経過が漏洩しても秘密情報は漏洩しないスカラー倍計算方法の第１実施例を示す図である。図１は、第１実施例のスカラー倍計算方法を示すフローチャートである。図１及び図２を参照して、第１実施例を説明する。

【００３１】

スカラー倍計算装置２０１では、点及びスカラー値２０７を入力し、以下の手順でスカラー倍２０８を出力する。ここで入力された点をＰ、入力されたスカラー値をｄ、出力するスカラー倍の点をｄＰで、それぞれ表すことにする。

【００３２】

ステップ１０１として、繰り返し判定部２０６において繰り返すか否かの判定を行なう為に、初期値として変数Ｉに１を代入する。ステップ１０２として、２倍算演算部２０４により、点Ｐの２倍点２Ｐを計算する。ステップ１０３として、スカラー倍計算装置２０１に入力された点Ｐとステップ１０２で求めた点２Ｐを、点格納部２０２に点の組（Ｐ，２Ｐ）として格納する。ステップ１０４として、繰り返し判定部２０６により、変数Ｉとスカラー値のビット長とが一致するかどうかを判定し、一致すればステップ１１３へ行く。一致しなければステップ１０５へ行く。ステップ１０５として、変数Ｉを１増加させる。ステップ１０６として、ビット値判定部２０５により、スカラー値のＩ番目のビットの値が０であるか１であるかを判定する。そのビットの値が０であればステップ１０７へ行く。そのビットの値が１であればステップ１１０へ行く。

【００３３】

ステップ１０７として、加算演算部２０３により、点格納部２０２に格納されている点の組（ｍＰ，（ｍ＋１）Ｐ）から点ｍＰと点（ｍ＋１）Ｐの加算ｍＰ＋（ｍ＋１）Ｐを行ない、点（２ｍ＋１）Ｐを計算する。その後ステップ１０８へ行く。ステップ１０８として、２倍算演算部２０４により、点格納部２０２に格納されている点の組（ｍＰ，（ｍ＋１）Ｐ）から点ｍＰの２倍算２（ｍＰ）を行ない、点２ｍＰを計算する。その後ステップ１０９へ行く。ステップ１０９として、ステップ１０８で求めた点２ｍＰとステップ１０７で求めた点（２ｍ＋１）Ｐを点格納部２０２に点の組（２ｍＰ，（２ｍ＋１）Ｐ）として、点の組（ｍＰ，（ｍ＋１）Ｐ）の代わりに格納する。その後ステップ１０４へ戻る。

【００３４】

ステップ１１０として、加算演算部２０３により、点格納部２０２に格納されている点の組（ｍＰ，（ｍ＋１）Ｐ）から点ｍＰと点（ｍ＋１）Ｐの加算ｍＰ＋（ｍ＋１）Ｐを行ない、点（２ｍ＋１）Ｐを計算する。その後ステップ１１１へ行く。ステップ１１１として、２倍算演算部２０４により、点格納部２０２に格納されている点の組（ｍＰ，（ｍ＋１）Ｐ）から点（ｍ＋１）Ｐの２倍算２（（ｍ＋１）Ｐ）を行ない、点（２ｍ＋２）Ｐを計算する。その後ステップ１１２へ行く。ステップ１１２として、ステップ１１０で求めた点（２ｍ＋１）Ｐとステップ１１１で求めた点（２ｍ＋２）Ｐを点格納部２０２に点の組（（２ｍ＋１）Ｐ，（２ｍ＋２）Ｐ）として、点の組（ｍＰ，（ｍ＋１）Ｐ）の代わりに格納する。その後ステップ１０４へ戻る。

【００３５】

ステップ１１３として、点格納部２０２に格納されている点の組（ｍＰ，（ｍ＋１）Ｐ）から、点ｍＰをスカラー倍２０８として出力し、終了する。

【００３６】

以上の手順により出力する値である点ｍＰが点Ｐのスカラー値ｄによるスカラー倍の点ｄＰとなることは、計算過程において格納されている点の組（ｍＰ，（ｍ＋１）Ｐ）の点ｍＰに対するスカラー値ｍが、スカラー値ｄにおける先頭Ｉビットのビット列と一致することと、ステップ１０４においてステップ１１３へ行くと判定されるためには、Ｉとスカラー値ｄのビット長が等しいことが必要であ

り、そのためスカラー値ｍとスカラー値ｄが一致することにより示される。

【００３７】

また、以上の手順によりスカラー倍計算経過が漏洩しても秘密情報であるスカラー値に関する情報が漏洩しないことの根拠は以下の通りである。計算経過からスカラー値に関する情報を得る為には、少なくとも、各々のスカラー値に対する計算経過の間に違いが存在しなければならない。まず、あるスカラー値と、そのスカラー値との間に特定のビットのみが異なるスカラー値とについて考える。特定ビットが異なるので、計算経過において特定の回数だけ繰り返した後のステップ１０６でのビット値の判定の後、ステップ１０７へ行くかステップ１１０へ行くかの違いが生じる。しかしながら、ステップ１０７へ行ってもステップ１１０へ行っても、共にその後で加算を行ない、次に２倍算を行ない、そしてその結果を点の組として格納するという手順をとり、ステップ１０４へと戻る為、計算経過としての差異は存在しない。したがって同一の計算経過をとるためスカラー値の情報は引き出すことはできない。

【００３８】

次に固定したビット長のスカラー値について考える。二つのビット長の同じスカラー値はいくつかのビットの値が異なる。値の異なるビットの数をｋとし、与えられた２つのスカラー値をそれぞれd_0及びd_kとする。スカラー値d_0とスカラー値d_kの間でビットの値が異なる最初のビットに対して、その値がd_kの対応するビットの値と等しく、その他のビットの値がd_0の対応するビットの値と等しいようなスカラー値をd_1とする。スカラー値d_0とスカラー値d_1は１ビットのみ値が異なる。次にスカラー値d_1とスカラー値d_kの間でビットの値が異なる最初のビットに対して、その値がd_kの対応するビットの値と等しく、その他のビットの値がd_1の対応するビットの値と等しいようなスカラー値をd_2とする。スカラー値d_1とスカラー値d_2は１ビットのみ値が異なる。以下同様にしてスカラー値d_{k-1}まで定める。スカラー値d_0とスカラー値d_kはｋビットの値が異なるので、スカラー値d_{k-1}とスカラー値d_kは１ビットのみ値が異なる。したがって下付き指数の値が１だけ異なるスカラー値同士は１ビットのみ値が異なる。上述したように、１ビットのみ値の異なるスカラー値同士に

おいてはそれらの計算経過は同一となる。スカラー値d_0からスカラー値d_kまで１ビットのみ値の異なるスカラー値の連鎖が存在するので、スカラー値d_0とスカラー値d_kの計算経過は同一となる。ゆえに計算経過によりスカラー値の情報を引き出すことはできない。

【００３９】

また、楕円曲線としてモンゴメリ型楕円曲線を用いると、加算及び２倍算が高速に実行可能であり、通常用いる標準型楕円曲線よりも高速にスカラー倍計算が実行可能である。

【００４０】

標数２の有限体上で定義された楕円曲線に対しても、高速な加算及び２倍算の計算方法が知られており、上記手順において加算及び２倍算の計算にその計算方法を用いることにより、標数２の有限体上で定義された楕円曲線の通常のスカラー倍計算と比べて、高速にスカラー倍計算が実行可能である。

【００４１】

図５は、図１１の暗号処理システム１１０１における秘密情報を用いた暗号処理において、暗号処理経過が漏洩しても秘密情報は漏洩しないスカラー倍計算方法の第２実施例を示す図である。図４は、第２実施例のスカラー倍計算方法を示すフローチャートである。図４及び図５を参照して、第２実施例を説明する。

【００４２】

スカラー倍計算装置５０１では、点及びスカラー値５０７を入力し、以下の手順でスカラー倍５０８を出力する。ステップ４０１として、繰り返し判定部５０６において繰り返すか否かの判定を行なう為に、初期値として変数Ｉに１を代入する。ステップ４０２として、２倍算演算部５０４により、点Ｐの２倍点２Ｐを計算する。ステップ４０３として、スカラー倍計算装置５０１に入力された点Ｐとステップ４０２で求めた点２Ｐを、点格納部５０２に点の組（Ｐ，２Ｐ）として格納する。ステップ４０４として、繰り返し判定部５０６により、変数Ｉとスカラー値のビット長とが一致するかどうかを判定し、一致すればステップ４１３へ行く。一致しなければステップ４０５へ行く。ステップ４０５として、変数Ｉを１増加させる。ステップ４０６として、ビット値判定部５０５により、スカラ

ー値のＩ番目のビットの値が０であるか１であるかを判定する。そのビットの値が０であればステップ４０７へ行く。そのビットの値が１であればステップ４１０へ行く。

【００４３】

ステップ４０７として、２倍算演算部５０４により、点格納部５０２に格納されている点の組（ｍＰ，（ｍ＋１）Ｐ）から点ｍＰの２倍算２（ｍＰ）を行ない、点２ｍＰを計算する。その後ステップ４０８へ行く。ステップ４０８として、加算演算部５０３により、点格納部５０２に格納されている点の組（ｍＰ，（ｍ＋１）Ｐ）から点ｍＰと点（ｍ＋１）Ｐの加算ｍＰ＋（ｍ＋１）Ｐを行ない、点（２ｍ＋１）Ｐを計算する。その後ステップ４０９へ行く。ステップ４０９として、ステップ４０７で求めた点２ｍＰとステップ４０８で求めた点（２ｍ＋１）Ｐを点格納部５０２に点の組（２ｍＰ，（２ｍ＋１）Ｐ）として、点の組（ｍＰ，（ｍ＋１）Ｐ）の代わりに格納する。その後ステップ４０４へ戻る。

【００４４】

ステップ４１０として、２倍算演算部５０４により、点格納部５０２に格納されている点の組（ｍＰ，（ｍ＋１）Ｐ）から点（ｍ＋１）Ｐの２倍算２（（ｍ＋１）Ｐ）を行ない、点（２ｍ＋２）Ｐを計算する。その後ステップ４１１へ行く。ステップ４１１として、加算演算部５０３により、点格納部５０２に格納されている点の組（ｍＰ，（ｍ＋１）Ｐ）から点ｍＰと点（ｍ＋１）Ｐの加算ｍＰ＋（ｍ＋１）Ｐを行ない、点（２ｍ＋１）Ｐを計算する。その後ステップ４１２へ行く。ステップ４１２として、ステップ４１１で求めた点（２ｍ＋１）Ｐとステップ４１０で求めた点（２ｍ＋２）Ｐを点格納部５０２に点の組（（２ｍ＋１）Ｐ，（２ｍ＋２）Ｐ）として、点の組（ｍＰ，（ｍ＋１）Ｐ）の代わりに格納する。その後ステップ４０４へ戻る。

【００４５】

ステップ４１３として、点格納部５０２に格納されている点の組（ｍＰ，（ｍ＋１）Ｐ）から、点ｍＰをスカラー倍５０８として出力し、終了する。

【００４６】

以上の手順により出力する値である点ｍＰが点Ｐのスカラー値ｄによるスカラ

ー倍の点ｄＰとなることは、第１実施例の場合と同様に示すことができる。

【００４７】

また、以上の手順によりスカラー倍計算経過が漏洩しても秘密情報であるスカラー値に関する情報が漏洩しないことの根拠は以下の通りである。ある特定のビットのみ値が異なる二つのスカラー値に対して、それらの計算経過が同一であることを示せば、他の部分は第一実施例における根拠と同様であるので、スカラー倍計算経過が漏洩しても秘密情報であるスカラー値に関する情報が漏洩しないことが示される。したがって、ある特定のビットのみ値が異なる二つのスカラー値について考える。ある特定のビットの値のみが異なるので、計算経過において特定の回数だけ繰り返した後のステップ４０６でのビット値の判定の後、ステップ４０７へ行くかステップ４１０へ行くかの違いが生じる。しかしながらステップ４０７へ行ってもステップ４１０へ行っても、共にその後で２倍算を行ない、次に加算を行ない、そしてその結果を点の組として格納するという手順をとり、ステップ４０４へと戻る為、計算経過としての差異は存在しない。ゆえにスカラー倍計算経過によりスカラー値の情報を引き出すことはできない。

【００４８】

また、楕円曲線としてモンゴメリ型楕円曲線を用いると、標準型楕円曲線よりも高速にスカラー倍計算が実行可能であることも、第１実施例と同様である。

【００４９】

標数２の有限体上で定義された楕円曲線に対しても、上記手順において加算及び２倍算の計算に高速な加算及び２倍算の計算方法を用いることにより、標数２の有限体上で定義された楕円曲線の通常のスカラー倍計算と比べて、高速にスカラー倍計算が実行可能であることも、第１実施例と同様である。

【００５０】

図７は、図１１の暗号処理システム１１０１における秘密情報を用いた暗号処理において、暗号処理経過が漏洩しても秘密情報は漏洩しないスカラー倍計算方法の第３実施例を示す図である。図６は、第３実施例のスカラー倍計算方法を示すフローチャートである。図６及び図７を参照して、第３実施例を説明する。

【００５１】

スカラー倍計算装置７０１では、点及びスカラー値７０７を入力し、以下の手順でスカラー倍７０８を出力する。ステップ６０１として、繰り返し判定部７０６において繰り返すか否かの判定を行なう為に、初期値として変数Ｉに１を代入する。ステップ６０２として、２倍算演算部７０４により、点Ｐの２倍点２Ｐを計算する。ステップ６０３として、スカラー倍計算装置７０１に入力された点Ｐとステップ６０２で求めた点２Ｐを、点格納部７０２に点の組（Ｐ，２Ｐ）として格納する。ステップ６０４として、繰り返し判定部７０６により、変数Ｉとスカラー値のビット長とが一致するかどうかを判定し、一致すればステップ６１３へ行く。一致しなければステップ６０５へ行く。ステップ６０５として、変数Ｉを１増加させる。ステップ６０６として、ビット値判定部７０５により、スカラー値のＩ番目のビットの値が０であるか１であるかを判定する。そのビットの値が０であればステップ６０７へ行く。そのビットの値が１であればステップ６１０へ行く。

【００５２】

ステップ６０７として、加算及び２倍算演算部７０３により、点格納部７０２に格納されている点の組（ｍＰ，（ｍ＋１）Ｐ）から点ｍＰと点（ｍ＋１）Ｐの加算ｍＰ＋（ｍ＋１）Ｐ及び点ｍＰの２倍算２（ｍＰ）を同時に行ない、点（２ｍ＋１）Ｐ及び点２ｍＰを計算する。その後ステップ６０９へ行く。ステップ６０９として、ステップ６０７で求めた点２ｍＰと点（２ｍ＋１）Ｐを点格納部７０２に点の組（２ｍＰ，（２ｍ＋１）Ｐ）として、点の組（ｍＰ，（ｍ＋１）Ｐ）の代わりに格納する。その後ステップ６０４へ戻る。

【００５３】

ステップ６１０として、加算及び２倍算演算部７０３により、点格納部７０２に格納されている点の組（ｍＰ，（ｍ＋１）Ｐ）から点ｍＰと点（ｍ＋１）Ｐの加算ｍＰ＋（ｍ＋１）Ｐ及び点（ｍ＋１）Ｐの２倍算２（（ｍ＋１）Ｐ）を同時に行ない、点（２ｍ＋１）Ｐ及び点（２ｍ＋２）Ｐを計算する。その後ステップ６１２へ行く。ステップ６１２として、ステップ６１０で求めた点（２ｍ＋１）Ｐと点（２ｍ＋２）Ｐを点格納部７０２に点の組（（２ｍ＋１）Ｐ，（２ｍ＋２）Ｐ）として、点の組（ｍＰ，（ｍ＋１）Ｐ）の代わりに格納する。その後ステ

ップ６０４へ戻る。

【００５４】

ステップ６１３として、点格納部７０２に格納されている点の組（ｍＰ，（ｍ＋１）Ｐ）から、点ｍＰをスカラー倍７０８として出力し、終了する。

【００５５】

以上の手順により出力する値である点ｍＰが点Ｐのスカラー値ｄによるスカラー倍の点ｄＰとなることは、第１実施例の場合と同様に示すことができる。

【００５６】

また、以上の手順によりスカラー倍計算経過が漏洩しても秘密情報であるスカラー値に関する情報が漏洩しないことの根拠は以下の通りである。ある特定のビットのみ値が異なる二つのスカラー値に対して、それらの計算経過が同一であることを示せば、他の部分は第一実施例における根拠と同様であるので、スカラー倍計算経過が漏洩しても秘密情報であるスカラー値に関する情報が漏洩しないことが示される。したがって、ある特定のビットのみ値が異なる二つのスカラー値について考える。ある特定のビットの値のみが異なるので、計算経過において特定の回数だけ繰り返した後のステップ６０６でのビット値の判定の後、ステップ６０７へ行くかステップ６１０へ行くかの違いが生じる。しかしながらステップ６０７へ行ってもステップ６１０へ行っても、共にその後で加算及び２倍算を同時に行ない、そしてそれらの結果を点の組として格納するという手順をとり、ステップ６０４へと戻る為、計算経過としての差異は存在しない。ゆえにスカラー倍計算経過によりスカラー値の情報を引き出すことはできない。

【００５７】

また、楕円曲線としてモンゴメリ型楕円曲線を用いると、標準型楕円曲線よりも高速にスカラー倍計算が実行可能であることも、第１実施例と同様である。

【００５８】

標数２の有限体上で定義された楕円曲線に対しても、上記手順において加算及び２倍算の計算に高速な加算及び２倍算の計算方法を用いることにより、標数２の有限体上で定義された楕円曲線の通常のスカラー倍計算と比べて、高速にスカラー倍計算が実行可能であることも、第１実施例と同様である。

【００５９】

図９は、図１１の暗号処理システム１１０１における秘密情報を用いた暗号処理において、暗号処理経過が漏洩しても秘密情報は漏洩しないスカラー倍計算方法の第４実施例を示す図である。図８は、第４実施例のスカラー倍計算方法を示すフローチャートである。図８及び図９を参照して、第４実施例を説明する。

【００６０】

スカラー倍計算装置９０１では、点及びスカラー値９０７を入力し、以下の手順でスカラー倍９０８を出力する。ステップ８０１として、繰り返し判定部９０６において繰り返すか否かの判定を行なう為に、初期値として変数Ｉに１を代入する。ステップ８０２として、２倍算演算部９０４により、点Ｐの２倍点２Ｐを計算する。ステップ８０３として、スカラー倍計算装置９０１に入力された点Ｐとステップ８０２で求めた点２Ｐを、点格納部９０２に点の組（Ｐ，２Ｐ）として格納する。ステップ８０４として、繰り返し判定部９０６により、変数Ｉとスカラー値のビット長とが一致するかどうかを判定し、一致すればステップ８１３へ行く。一致しなければステップ８０５へ行く。ステップ８０５として、変数Ｉを１だけ増加させる。ステップ８０６として、加算演算部９０３により、点格納部９０２に格納されている点の組（ｍＰ，（ｍ＋１）Ｐ）から点ｍＰと点（ｍ＋１）Ｐの加算ｍＰ＋（ｍ＋１）Ｐを行ない、点（２ｍ＋１）Ｐを計算する。ステップ８０７として、ビット値判定部９０５により、スカラー値のＩ番目のビットの値が０であるか１であるかを判定する。そのビットの値が０であればステップ８０８へ行く。そのビットの値が１であればステップ８１１へ行く。

【００６１】

ステップ８０８として、２倍算演算部９０４により、点格納部９０２に格納されている点の組（ｍＰ，（ｍ＋１）Ｐ）から点ｍＰの２倍算２（ｍＰ）を行ない、点２ｍＰを計算する。その後ステップ８０９へ行く。ステップ８０９として、ステップ８０８で求めた点２ｍＰとステップ８０６で求めた点（２ｍ＋１）Ｐを点格納部９０２に点の組（２ｍＰ，（２ｍ＋１）Ｐ）として、点の組（ｍＰ，（ｍ＋１）Ｐ）の代わりに格納する。その後ステップ８０４へ戻る。ステップ８１１として、２倍算演算部９０４により、点格納部９０２に格納されている点の組

（ｍＰ，（ｍ＋１）Ｐ）から点（ｍ＋１）Ｐの２倍算２（（ｍ＋１）Ｐ）を行ない、点（２ｍ＋２）Ｐを計算する。その後ステップ８１２へ行く。ステップ８１２として、ステップ８０６で求めた点（２ｍ＋１）Ｐとステップ８１１で求めた点（２ｍ＋２）Ｐを点格納部９０２に点の組（（２ｍ＋１）Ｐ，（２ｍ＋２）Ｐ）として、点の組（ｍＰ，（ｍ＋１）Ｐ）の代わりに格納する。その後ステップ８０４へ戻る。

【００６２】

ステップ８１３として、点格納部９０２に格納されている点の組（ｍＰ，（ｍ＋１）Ｐ）から、点ｍＰをスカラー倍９０８として出力し、終了する。

【００６３】

以上の手順により出力する値である点ｍＰが点Ｐのスカラー値ｄによるスカラー倍の点ｄＰとなることは、第１実施例の場合と同様に示すことができる。

【００６４】

また、以上の手順によりスカラー倍計算経過が漏洩しても秘密情報であるスカラー値に関する情報が漏洩しないことの根拠は以下の通りである。ある特定のビットのみ値が異なる二つのスカラー値に対して、それらの計算経過が同一であることを示せば、他の部分は第一実施例における根拠と同様であるので、スカラー倍計算経過が漏洩しても秘密情報であるスカラー値に関する情報が漏洩しないことが示される。したがって、ある特定のビットのみ値が異なる二つのスカラー値について考える。ある特定のビットの値のみが異なるので、計算経過において特定の回数だけ繰り返した後のステップ８０７でのビット値の判定の後、ステップ８０８へ行くかステップ８１１へ行くかの違いが生じる。しかしながらステップ８０８へ行ってもステップ８１１へ行っても、共にその後で２倍算を行ない、そしてその結果を加算の結果とともに点の組として格納するという手順をとり、ステップ８０４へと戻る為、計算経過としての差異は存在しない。ゆえにスカラー倍計算経過によりスカラー値の情報を引き出すことはできない。

【００６５】

また、楕円曲線としてモンゴメリ型楕円曲線を用いると、標準型楕円曲線よりも高速にスカラー倍計算が実行可能であることも、第１実施例と同様である。

【００６６】

標数２の有限体上で定義された楕円曲線に対しても、上記手順において加算及び２倍算の計算に高速な加算及び２倍算の計算方法を用いることにより、標数２の有限体上で定義された楕円曲線の通常のスカラー倍計算と比べて、高速にスカラー倍計算が実行可能であることも、第１実施例と同様である。

【００６７】

図１５は、図１１の暗号処理システム１１０１における秘密情報を用いた暗号処理において、暗号処理経過が漏洩しても秘密情報は漏洩しないスカラー倍計算方法の第５実施例を示す図である。図１２、図１３及び図１４は、第５実施例のスカラー倍計算方法を示すフローチャートである。図１２～図１５を参照して、第５実施例を説明する。

【００６８】

スカラー倍計算装置１５０１では、点及びスカラー値１５０７を入力し、以下の手順でスカラー倍１５０８を出力する。ステップ１２０１として、繰り返し判定部１５０６において繰り返すか否かの判定を行なう為に、初期値として変数Ｉに１を代入する。ステップ１２０２として、２倍算演算部１５０４により、点Ｐの２倍点２Ｐを計算する。ステップ１２０３として、スカラー倍計算装置１５０１に入力された点Ｐとステップ１２０２で求めた点２Ｐを、点格納部１５０２に点の組（Ｐ，２Ｐ）として格納する。ステップ１２０４として、繰り返し判定部１５０６により、変数Ｉとスカラー値のビット長とが一致するかどうかを判定し、一致すればステップ１２１３へ行く。一致しなければステップ１２０５へ行く。ステップ１２０５として、変数Ｉを１増加させる。ステップ１２０６として、演算ランダム化部１５０９により、加算及び２倍算の計算順序をランダム化する。加算、２倍算の順序で計算を実行する場合はステップ１３０１へ行く。２倍算、加算の順序で計算を実行する場合はステップ１４０１へ行く。

【００６９】

ステップ１３０１として、ビット値判定部１５０５により、スカラー値のＩ番目のビットの値が０であるか１であるかを判定する。そのビットの値が０であればステップ１３０２へ行く。そのビットの値が１であればステップ１３０５へ行

の計算順序をランダム化する。加算、２倍算の順序で計算を実行する場合はステップ２４０５へ行く。２倍算、加算の順序で計算を実行する場合はステップ２４０２へ行く。

【００８７】

ステップ２４０２として、２倍算演算部２５０４により、点格納部２５０２に格納されている点の組（ｍＰ，（ｍ＋１）Ｐ）から点ｍＰの２倍算２（ｍＰ）を行ない、点２ｍＰを計算する。その後ステップ２４０３へ行く。ステップ２４０３として、加算演算部２５０３により、点格納部２５０２に格納されている点の組（ｍＰ，（ｍ＋１）Ｐ）から点ｍＰと点（ｍ＋１）Ｐの加算ｍＰ＋（ｍ＋１）Ｐを行ない、点（２ｍ＋１）Ｐを計算する。その後ステップ２４０４へ行く。

【００８８】

ステップ２４０５として、加算演算部２５０３により、点格納部２５０２に格納されている点の組（ｍＰ，（ｍ＋１）Ｐ）から点ｍＰと点（ｍ＋１）Ｐの加算ｍＰ＋（ｍ＋１）Ｐを行ない、点（２ｍ＋１）Ｐを計算する。その後ステップ２４０６へ行く。ステップ２４０６として、２倍算演算部２５０４により、点格納部２５０２に格納されている点の組（ｍＰ，（ｍ＋１）Ｐ）から点ｍＰの２倍算２（ｍＰ）を行ない、点２ｍＰを計算する。その後ステップ２４０４へ行く。

【００８９】

ステップ２４０４として、ステップ２４０２乃至はステップ２４０６で求めた点２ｍＰとステップ２４０３乃至はステップ２４０５で求めた点（２ｍ＋１）Ｐを点格納部２５０２に点の組（２ｍＰ，（２ｍ＋１）Ｐ）として、点の組（ｍＰ，（ｍ＋１）Ｐ）の代わりに格納する。その後ステップ２２０４へ戻る。

【００９０】

ステップ２２１３として、点格納部２５０２に格納されている点の組（ｍＰ，（ｍ＋１）Ｐ）から、点ｍＰをスカラー倍２５０８として出力し、終了する。

【００９１】

以上の手順により出力する値である点ｍＰが点Ｐのスカラー値ｄによるスカラー倍の点ｄＰとなることは、第１実施例の場合と同様に示すことができる。

【００９２】

また、楕円曲線としてモンゴメリ型楕円曲線を用いると、加算及び２倍算が高速に実行可能であり、通常用いる標準型楕円曲線よりも高速にスカラー倍計算が実行可能である。

【００９３】

標数２の有限体上で定義された楕円曲線に対しても、上記手順において加算及び２倍算の計算に高速な加算及び２倍算の計算方法を用いることにより、標数２の有限体上で定義された楕円曲線の通常のスカラー倍計算と比べて、高速にスカラー倍計算が実行可能である。

【００９４】

図２７は、図１１の暗号処理システム１１０１における秘密情報を用いた暗号処理において、暗号処理経過が漏洩しても秘密情報は漏洩しないスカラー倍計算方法の第７実施例を示す図である。図２６は、第７実施例のスカラー倍計算方法を示すフローチャートである。図２６及び図２７を参照して、第７実施例を説明する。

【００９５】

スカラー倍計算装置２７０１では、点及びスカラー値２７０７を入力し、以下の手順でスカラー倍２７０８を出力する。ステップ２６０１として、繰り返し判定部２７０６において繰り返すか否かの判定を行なう為に、初期値として変数Ｉに１を代入する。ステップ２６１４として、ランダム化射影座標変換部２７０９により、乱数ｋを生成する。ステップ２６１５として、ランダム化射影座標変換部２７０９により、ステップ２６１４で生成したｋを用いて、点Ｐを射影座標において、Ｐ＝（ｋｘ，ｋｙ，ｋ）と表す。ここで点Ｐは、アフィン座標では、Ｐ＝（ｘ，ｙ）と表されるとする。ステップ２６０２として、２倍算演算部２７０４により、ステップ２６１５で（ｋｘ，ｋｙ，ｋ）と表された点Ｐの２倍点２Ｐを計算する。ステップ２６０３として、スカラー倍計算装置２７０１に入力され、ステップ２６１５で（ｋｘ，ｋｙ，ｋ）と表された点Ｐと、ステップ２６０２で求めた点２Ｐを、点格納部２７０２に点の組（Ｐ，２Ｐ）として格納する。

【００９６】

ステップ２６０４として、繰り返し判定部２７０６により、変数Ｉとスカラー

値のビット長とが一致するかどうかを判定し、一致すればステップ２６１３へ行く。一致しなければステップ２６０５へ行く。ステップ２６０５として、変数Ｉを１増加させる。ステップ２６０６として、ビット値判定部２７０５により、スカラー値のＩ番目のビットの値が０であるか１であるかを判定する。そのビットの値が０であればステップ２６０７へ行く。そのビットの値が１であればステップ２６１０へ行く。

【００９７】

ステップ２６０７として、加算演算部２７０３により、点格納部２７０２に格納されている点の組（ｍＰ，（ｍ＋１）Ｐ）から点ｍＰと点（ｍ＋１）Ｐの加算ｍＰ＋（ｍ＋１）Ｐを行ない、点（２ｍ＋１）Ｐを計算する。その後ステップ２６０８へ行く。ステップ２６０８として、２倍算演算部２７０４により、点格納部２７０２に格納されている点の組（ｍＰ，（ｍ＋１）Ｐ）から点ｍＰの２倍算２（ｍＰ）を行ない、点２ｍＰを計算する。その後ステップ２６０９へ行く。ステップ２６０９として、ステップ２６０８で求めた点２ｍＰとステップ２６０７で求めた点（２ｍ＋１）Ｐを点格納部２７０２に点の組（２ｍＰ，（２ｍ＋１）Ｐ）として、点の組（ｍＰ，（ｍ＋１）Ｐ）の代わりに格納する。その後ステップ２６０４へ戻る。

【００９８】

ステップ２６１０として、加算演算部２７０３により、点格納部２７０２に格納されている点の組（ｍＰ，（ｍ＋１）Ｐ）から点ｍＰと点（ｍ＋１）Ｐの加算ｍＰ＋（ｍ＋１）Ｐを行ない、点（２ｍ＋１）Ｐを計算する。その後ステップ２６１１へ行く。ステップ２６１１として、２倍算演算部２７０４により、点格納部２７０２に格納されている点の組（ｍＰ，（ｍ＋１）Ｐ）から点（ｍ＋１）Ｐの２倍算２（（ｍ＋１）Ｐ）を行ない、点（２ｍ＋２）Ｐを計算する。その後ステップ２６１２へ行く。ステップ２６１２として、ステップ２６１０で求めた点（２ｍ＋１）Ｐとステップ２６１１で求めた点（２ｍ＋２）Ｐを点格納部２７０２に点の組（（２ｍ＋１）Ｐ，（２ｍ＋２）Ｐ）として、点の組（ｍＰ，（ｍ＋１）Ｐ）の代わりに格納する。その後ステップ２６０４へ戻る。

【００９９】

ステップ２６１３として、点格納部２７０２に格納されている点の組（ｍＰ，（ｍ＋１）Ｐ）から、点ｍＰをスカラー倍２７０８として出力し、終了する。

【０１００】

以上の手順により出力する値である点ｍＰが点Ｐのスカラー値ｄによるスカラー倍の点ｄＰとなることは、第１実施例の場合と同様に示すことができる。

【０１０１】

また、以上の手順によりスカラー倍計算経過が漏洩しても秘密情報であるスカラー値に関する情報が漏洩しないことの根拠は、第１実施例における根拠と同様である。そのうえ、スカラー倍計算において、特定の値が出現するか否かを観測し、そこからスカラー値を割り出す攻撃法に対しても、最初にランダムな値を乗じている為、特定の値の出現を予測できなくなるので、そのような攻撃法に対しても、スカラー値に関する情報が漏洩しないことがわかる。

【０１０２】

また、楕円曲線としてモンゴメリ型楕円曲線を用いると、標準型楕円曲線よりも高速にスカラー倍計算が実行可能であることも、第１実施例と同様である。

【０１０３】

標数２の有限体上で定義された楕円曲線に対しても、上記手順において加算及び２倍算の計算に高速な加算及び２倍算の計算方法を用いることにより、標数２の有限体上で定義された楕円曲線の通常のスカラー倍計算と比べて、高速にスカラー倍計算が実行可能であることも、第１実施例と同様である。

【０１０４】

図２８は、図２７のランダム化射影座標変換部２７０９として使用するランダム化射影座標変換装置の一実施例を示す図である。図２９は、このランダム化射影座標変換装置におけるランダム化射影座標変換方法を示すフローチャートである。

【０１０５】

ランダム化射影座標変換装置２８０１では、楕円曲線上の点２８０５を入力し、以下の手順でランダム化射影座標で表された点２８０６を出力する。ステップ２９０１として、座標判定部２８０２により、与えられた楕円曲線上の点２８０

５がアフィン座標で表されているか、それとも射影座標で表されているかを判定する。アフィン座標で表されていればステップ２９０２へ行く。射影座標で表されていればステップ２９０３へ行く。ステップ２９０２として、次のようにしてアフィン座標で表された点を射影座標で表す。アフィン座標で表された点を（ｘ，ｙ）とすると、射影座標として（ｘ，ｙ，１）と表す。

【０１０６】

ステップ２９０３として、乱数生成部２８０３により、乱数ｋを生成する。ステップ２９０４として、射影座標変換部２８０４により、次のようにして射影座標で表された与えられた点ををランダム化射影座標により表す。与えられた点を（ｘ，ｙ，ｚ）とすると、乱数生成部２８０３で生成された乱数ｋを、各座標に乗じ、（ｋｘ，ｋｙ，ｋｚ）と表し、ランダム化射影座標で表された点２８０６として出力する。

【０１０７】

射影座標においては、０以外の任意の数ｋにより各座標を乗じても、同じ点と見做す。すなわち、（ｘ，ｙ，ｚ）と（ｋｘ，ｋｙ，ｋｚ）は同じ点を表している。

【０１０８】

また、メモリ等の節約の為、ステップ２９０２の（ｘ，ｙ，１）は実際に格納しなくとも、仮想的に（ｘ，ｙ，１）と表されていると考え、ステップ２９０４で（ｋｘ，ｋｙ，ｋ）と表す際に、実際に格納を行なってもよい。

【０１０９】

図３は、図１１の本実施形態の暗号処理システムを署名作成装置として利用する場合の構成を示す。図１１における暗号処理部１１０２は、図３の署名作成装置３０１では署名部３０２になる。図１８は、図３の署名作成装置における処理の流れを示すフローチャートである。図１９は、図３の署名作成装置における処理の流れを示すシーケンス図である。

【０１１０】

図１８において、署名作成装置３０１は、以下のようにして、与えられたメッセージ３０５から署名が付随しているメッセージ３０６を出力する。メッセージ

３０５を署名作成装置３０１に入力すると、署名部３０２がそれを受け取る（ステップ１８０１）。署名部３０２は、スカラー倍計算部３０３に、入力メッセージ３０５に応じた楕円曲線上の点を与える（ステップ１８０２）。スカラー倍計算部３０３は、秘密情報格納部３０４より秘密情報であるスカラー値を受け取る（ステップ１８０３）。スカラー倍計算部３０３は、受け取った点とスカラー値より、スカラー倍点を、スカラー倍計算経過が漏洩しても秘密情報は漏洩しないスカラー倍計算方法で計算する（ステップ１８０４）。スカラー倍計算部３０３は、計算したスカラー倍点を署名部３０２に送る（ステップ１８０５）。署名部３０２は、スカラー倍計算部３０３より受け取ったスカラー倍点をもとにして署名作成処理を行なう（ステップ１８０６）。その結果を署名が付随したメッセージ３０６として出力する（ステップ１８０７）。

【０１１１】

上記処理手順を図１９のシーケンス図を用いて説明する。まず、署名部１９０１（図３の３０２）の実行する処理について説明する。署名部１９０１は、入力メッセージを受け取る。署名部１９０１は、入力メッセージをもとに楕円曲線上の点を選び、スカラー倍計算部１９０２に楕円曲線上の点を与え、そしてスカラー倍計算部１９０２からスカラー倍点を受け取る。署名部１９０１は、受け取ったスカラー倍点を用いて署名作成処理を行ない、その結果を出力メッセージとして出力する。

【０１１２】

次にスカラー倍計算部１９０２（図３の３０３）の実行する処理について説明する。スカラー倍計算部１９０２は、署名部１９０１より楕円曲線上の点を受け取る。スカラー倍計算部１９０２は、秘密情報格納部１９０３よりスカラー値を受け取る。スカラー倍計算部１９０３は、受け取った楕円曲線上の点及びスカラー値から、スカラー倍計算経過が漏洩しても秘密情報は漏洩しないスカラー倍計算方法により、スカラー倍点を計算し、署名部１９０１にスカラー倍点を送る。

【０１１３】

最後に秘密情報格納部１９０３（図３の３０４）の実行する処理について説明する。秘密情報格納部１９０３は、スカラー倍計算部１９０２がスカラー倍を計

算できるように、スカラー値をスカラー倍計算部１９０２に送る。

【０１１４】

スカラー倍計算部３０３が実行するスカラー倍計算は、上述した第１～第７実施例で説明したものがそのまま適用される。したがって、このスカラー倍計算は、スカラー倍計算経過が漏洩しても秘密情報であるスカラー値に関する情報は漏洩しないものである。そのため署名部３０２において、署名作成処理を行なう際に署名作成処理経過が漏洩したとしても、秘密情報であるスカラー値を扱っているのはスカラー倍計算部３０３のみであり、秘密情報に関する情報は漏洩しない。

【０１１５】

図１０は、図１１の本実施形態の暗号処理システムを復号化装置として利用する場合の構成を示す。図１１における暗号処理部１１０２は、図１０の復号化装置１００１では復号部１００２になる。図２０は、図１０の復号化装置における処理の流れを示すフローチャートである。図２１は、図１０の復号化装置における処理の流れを示すシーケンス図である。

【０１１６】

図２０において、復号化装置１００１は、以下のようにして、与えられたメッセージ１００５から復号化されたメッセージ１００６を出力する。メッセージ１００５を復号化装置１００１に入力すると、復号部１００２がそれを受け取る（ステップ２００１）。復号部１００２は、スカラー倍計算部１００３に、入力メッセージ１００５に応じた楕円曲線上の点を与える（ステップ２００２）。スカラー倍計算部１００３は、秘密情報格納部１００４より秘密情報であるスカラー値を受け取る（２００３）。スカラー倍計算部１００３は、受け取った点とスカラー値より、スカラー倍点を、スカラー倍計算経過が漏洩しても秘密情報は漏洩しないスカラー倍計算方法で計算する（ステップ２００４）。スカラー倍計算部１００３は、計算したスカラー倍点を復号部１００２に送る（ステップ２００５）。復号部１００２は、スカラー倍計算部１００３より受け取ったスカラー倍点をもとにして復号化処理を行なう（ステップ２００６）。その結果を復号化されたメッセージ１００６として出力する（ステップ２００７）。

【０１１７】

上記処理手順を図２１のシーケンス図を用いて説明する。まず、復号部２１０１（図１０の１００２）の実行する処理について説明する。復号部２１０１は、入力メッセージを受け取る。復号部２１０１は、入力メッセージをもとに楕円曲線上の点を選び、スカラー倍計算部２１０２に楕円曲線上の点を与え、そしてスカラー倍計算部２１０２からスカラー倍点を受け取る。復号部２１０１は、受け取ったスカラー倍点を用いて復号化処理を行ない、その結果を出力メッセージとして出力する。

【０１１８】

次にスカラー倍計算部２１０２（図１０の１００３）の実行する処理について説明する。スカラー倍計算部２１０２は、復号部２１０１より楕円曲線上の点を受け取る。スカラー倍計算部２１０２は、秘密情報格納部２１０３よりスカラー値を受け取る。スカラー倍計算部２１０３は、受け取った楕円曲線上の点及びスカラー値から、スカラー倍計算経過が漏洩しても秘密情報は漏洩しないスカラー倍計算方法により、スカラー倍点を計算し、復号部２１０１にスカラー倍点を送る。

【０１１９】

最後に秘密情報格納部２１０３（図１０の１００４）の実行する処理について説明する。秘密情報格納部２１０３は、スカラー倍計算部２１０２がスカラー倍を計算できるように、スカラー値をスカラー倍計算部２１０２に送る。

【０１２０】

スカラー倍計算部１００３が実行するスカラー倍計算は、上述した第１～第７実施例で説明したものがそのまま適用される。したがって、このスカラー倍計算は、スカラー倍計算経過が漏洩しても秘密情報であるスカラー値に関する情報は漏洩しないものである。そのため復号部１００２において、復号化処理を行なう際に復号化処理経過が漏洩したとしても、秘密情報であるスカラー値を扱っているのはスカラー倍計算部１００３のみであり、秘密情報に関する情報は漏洩しない。

【０１２１】

【発明の効果】

以上述べたように、本発明によれば、暗号処理システムにおける秘密情報を用いた暗号処理において、暗号処理経過が漏洩しても、暗号処理経過と秘密情報との依存関係が完全に断ち切られているので、秘密情報は漏洩しない。また、使用する楕円曲線をモンゴメリ型楕円曲線とすることで暗号処理の高速化を図ることができる。同様に、楕円曲線として標数２の有限体上で定義された楕円曲線を用いることで暗号処理の高速化を図ることができる。

【図面の簡単な説明】

【図１】

本発明の第１実施例のスカラー倍計算方法を示すフローチャート図である。

【図２】

第１実施例のスカラー倍計算方法及び装置における処理の流れを示す図である。

【図３】

本発明の実施の形態に係る署名作成装置の構成図である。

【図４】

本発明の第２実施例のスカラー倍計算方法を示すフローチャート図である。

【図５】

第２実施例のスカラー倍計算方法及び装置における処理の流れを示す図である。

【図６】

本発明の第３実施例のスカラー倍計算方法を示すフローチャート図である。

【図７】

第３実施例のスカラー倍計算方法及び装置における処理の流れを示す図である。

【図８】

本発明の第４実施例のスカラー倍計算方法を示すフローチャート図である。

【図９】

第４実施例のスカラー倍計算方法及び装置における処理の流れを示す図である

。

【図１０】

本発明の実施の形態に係る復号化装置の構成図である。

【図１１】

本発明の実施の形態に係る暗号処理システムの構成図である。

【図１２】

本発明の第５実施例のスカラー倍計算方法を示すフローチャート図である。

【図１３】

本発明の第５実施例のスカラー倍計算方法を示すフローチャート図である。

【図１４】

本発明の第５実施例のスカラー倍計算方法を示すフローチャート図である。

【図１５】

第５実施例のスカラー倍計算方法及び装置における処理の流れを示す図である

。

【図１６】

図１１の暗号処理システムにおける暗号処理方法を示すフローチャート図である。

【図１７】

図１１の暗号処理システムにおける処理の流れを示すシーケンス図である。

【図１８】

図３の署名作成装置における署名作成方法を示すフローチャート図である。

【図１９】

図３の署名作成装置における処理の流れを示すシーケンス図である。

【図２０】

図１０の復号化装置における復号化方法を示すフローチャート図である。

【図２１】

図１０の復号化装置での処理の流れを示すシーケンス図である。

【図２２】

本発明の第６実施例のスカラー倍計算方法を示すフローチャート図である。

【図２３】

本発明の第６実施例のスカラー倍計算方法を示すフローチャート図である。

【図２４】

本発明の第６実施例のスカラー倍計算方法を示すフローチャート図である。

【図２５】

第６実施例のスカラー倍計算方法及び装置における処理の流れを示す図である。

【図２６】

本発明の第７実施例のスカラー倍計算方法を示すフローチャート図である。

【図２７】

第７実施例のスカラー倍計算方法及び装置における処理の流れを示す図である。

【図２８】

図２７のランダム化射影座標変換装置を示す図である。

【図２９】

ランダム化射影座標変換装置におけるランダム化射影座標変換方法を示すフローチャート図である。

【符号の説明】

２０１　スカラー倍計算装置

２０２　点格納部

２０３　加算演算部

２０４　２倍算演算部

２０５　ビット値判定部

２０６　繰り返し判定部

２０７　点及びスカラー値

２０８　スカラー倍

３０１　署名作成装置

３０２　署名部

３０３　スカラー倍計算部

３０４　秘密情報格納部

３０５　入力メッセージ

３０６　出力メッセージ

７０１　スカラー倍計算装置

７０２　点格納部

７０３　加算及び２倍算演算部

７０４　２倍算演算部

７０５　ビット値判定部

７０６　繰り返し判定部

７０７　点及びスカラー値

７０８　スカラー倍

１００１　復号化装置

１００２　復号化部

１００３　スカラー倍計算部

１００４　秘密情報格納部

１００５　入力メッセージ

１００６　出力メッセージ

１１０１　暗号処理システム

１１０２　暗号処理部

１１０３　スカラー倍計算部

１１０４　秘密情報格納部

１１０５　入力メッセージ

１１０６　出力メッセージ

１５０１　スカラー倍計算装置

１５０２　点格納部

１５０３　加算演算部

１５０４　２倍算演算部

１５０５　ビット値判定部

１５０６　繰り返し判定部

１５０７　点及びスカラー値

１５０８　スカラー倍

１５０９　演算ランダム化部

２７０１　スカラー倍計算装置

２７０２　点格納部

２７０３　加算演算部

２７０４　２倍算演算部

２７０５　ビット値判定部

２７０６　繰り返し判定部

２７０７　点及びスカラー値

２７０８　スカラー倍

２７０９　ランダム化射影座標変換部

２８０１　ランダム化射影座標変換装置

２８０２　座標判定部

２８０３　乱数生成部

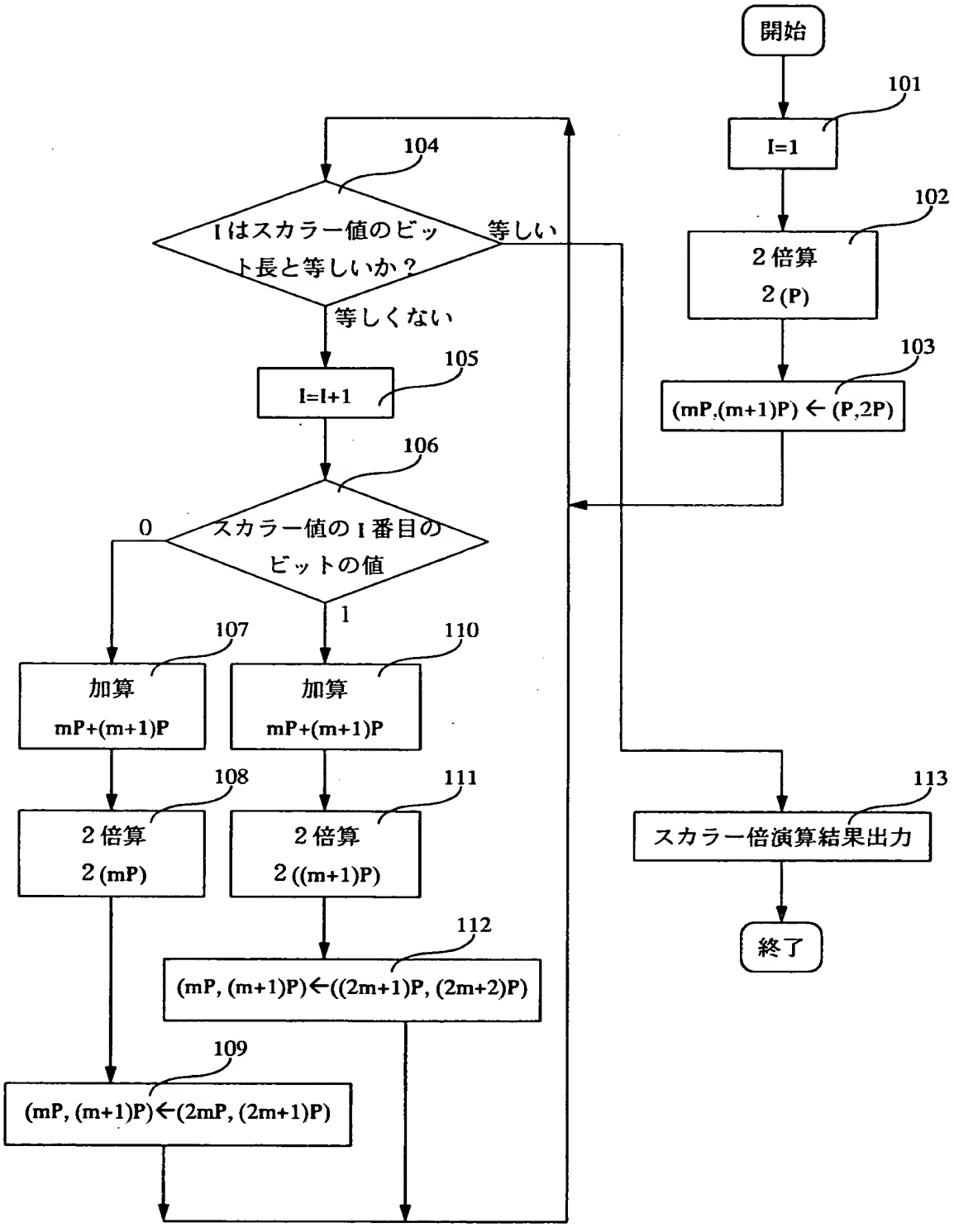
２８０４　射影座標変換部

２８０５　楕円曲線上の点

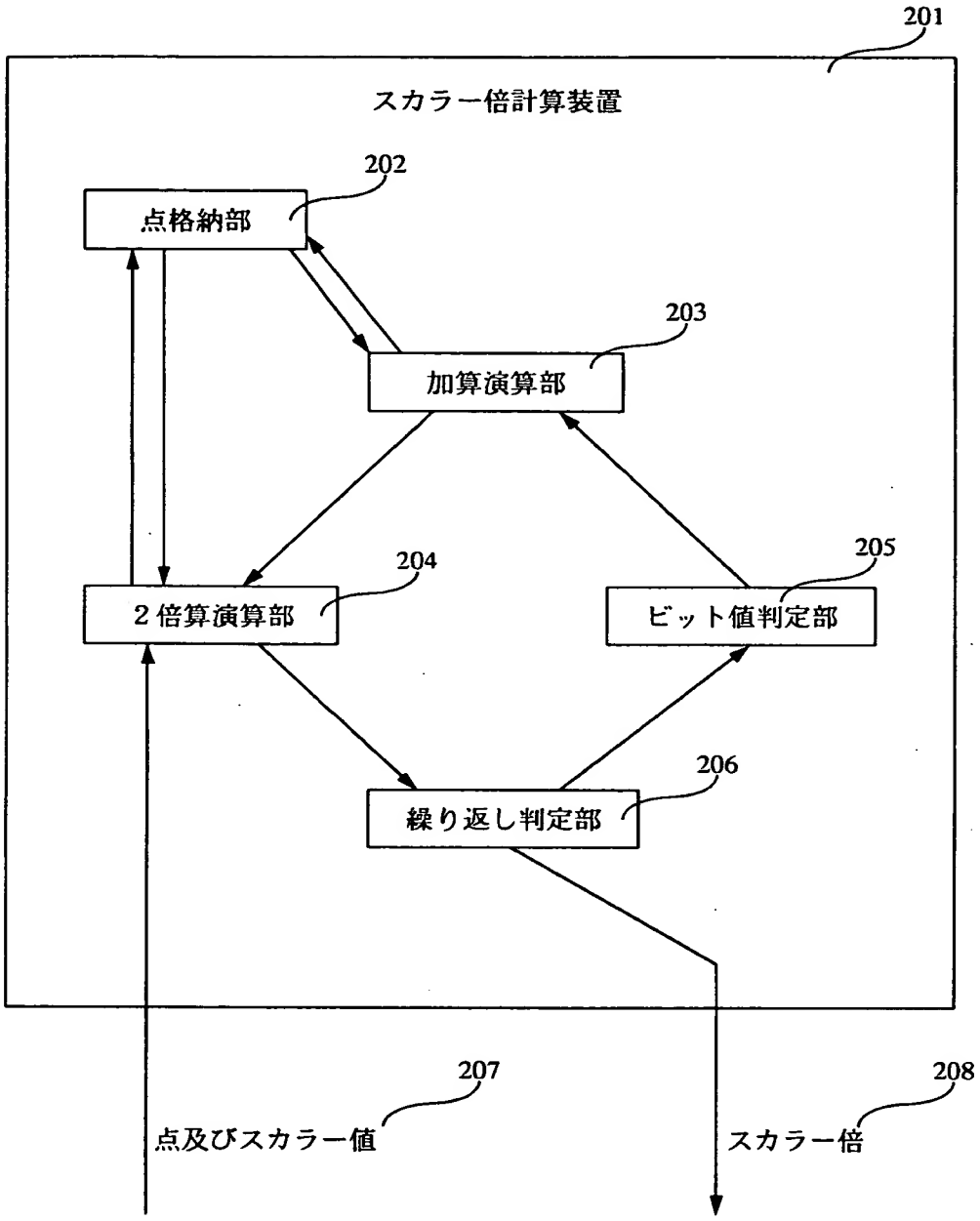
２８０６　ランダム化射影座標で表された点

【書類名】　図面

【図１】

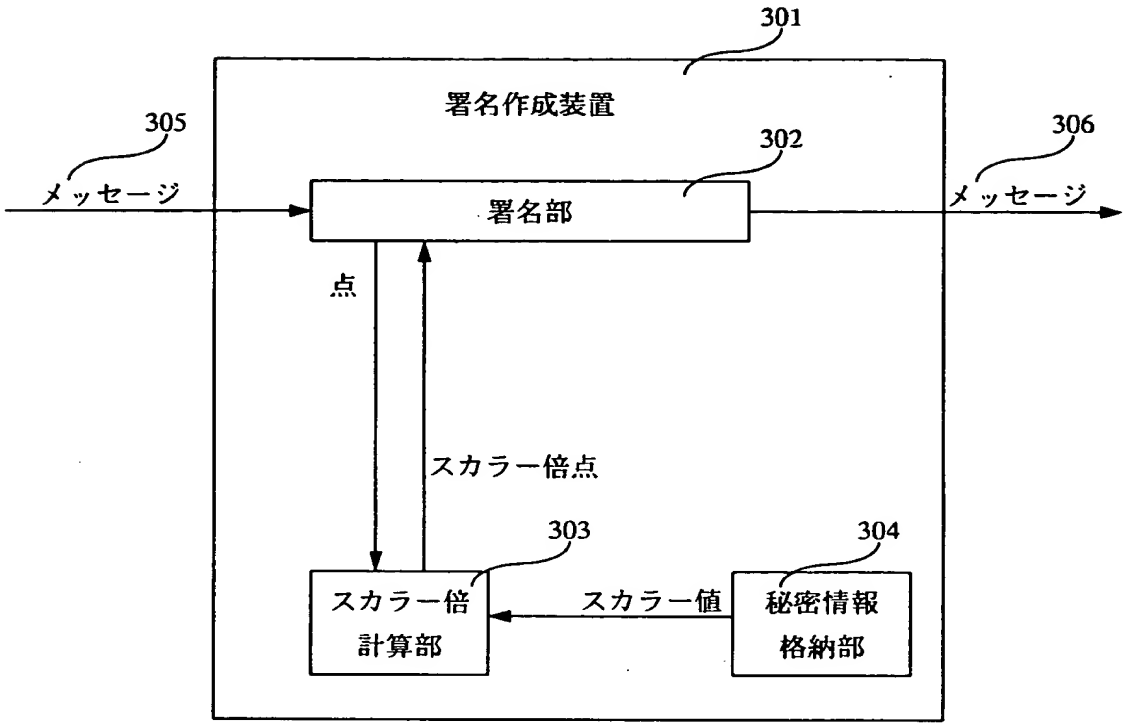

開始
101
I=1
102
２倍算
２(P)
103
(mP,(m+1)P) ← (P,2P)
104
Iはスカラー値のビット長と等しいか？
等しい
等しくない
105
I=I+1
106
スカラー値のI番目のビットの値
0
1
107
加算
mP+(m+1)P
110
加算
mP+(m+1)P
108
２倍算
２(mP)
111
２倍算
２((m+1)P)
112
(mP, (m+1)P)←((2m+1)P, (2m+2)P)
109
(mP, (m+1)P)←(2mP, (2m+1)P)
113
スカラー倍演算結果出力
終了

【図２】

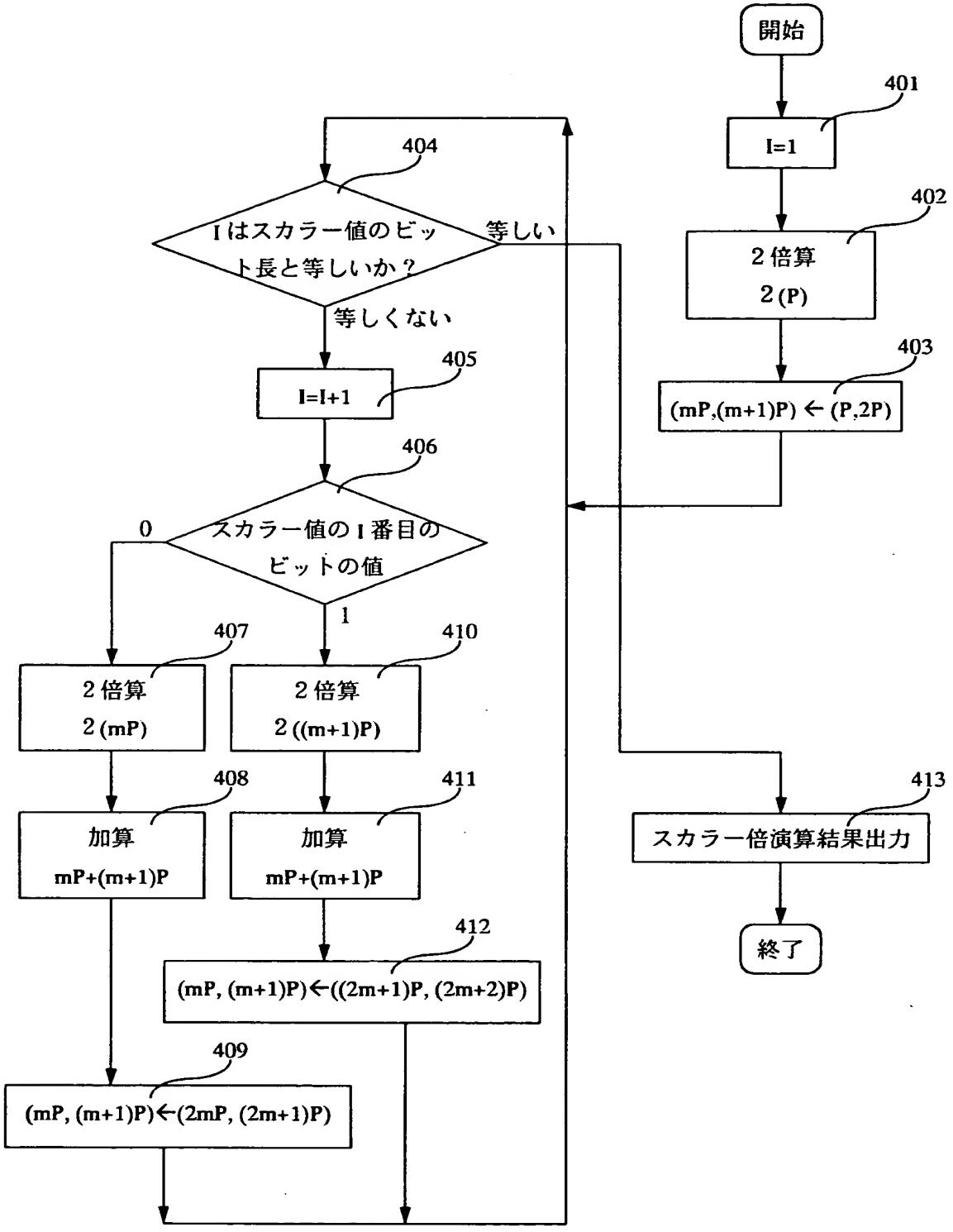


出証特２００１－３０１５４０３

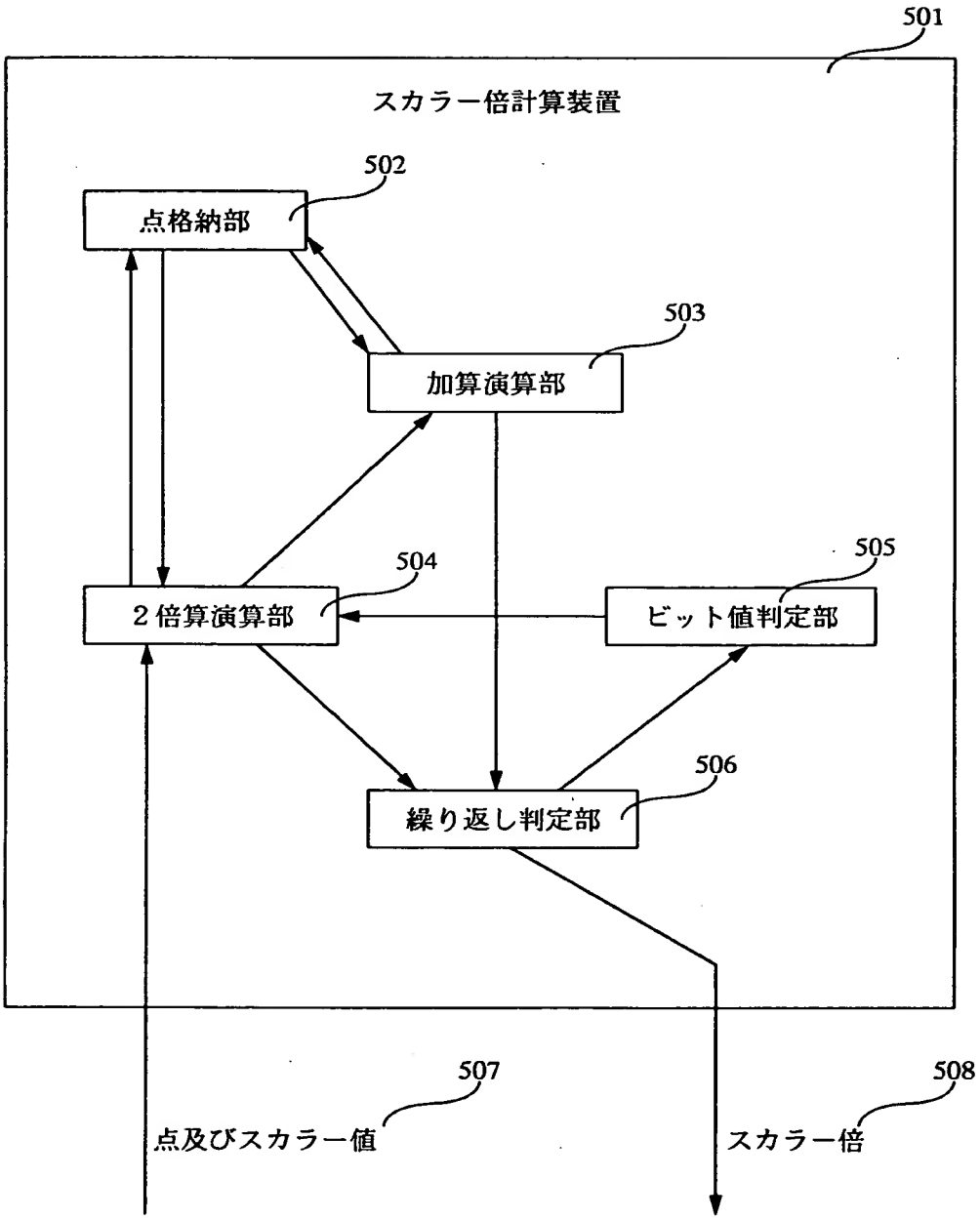
【図３】


301
署名作成装置
305
メッセージ
302
署名部
306
メッセージ
点
スカラー倍点
303
304
スカラー倍
計算部
スカラー値
秘密情報
格納部

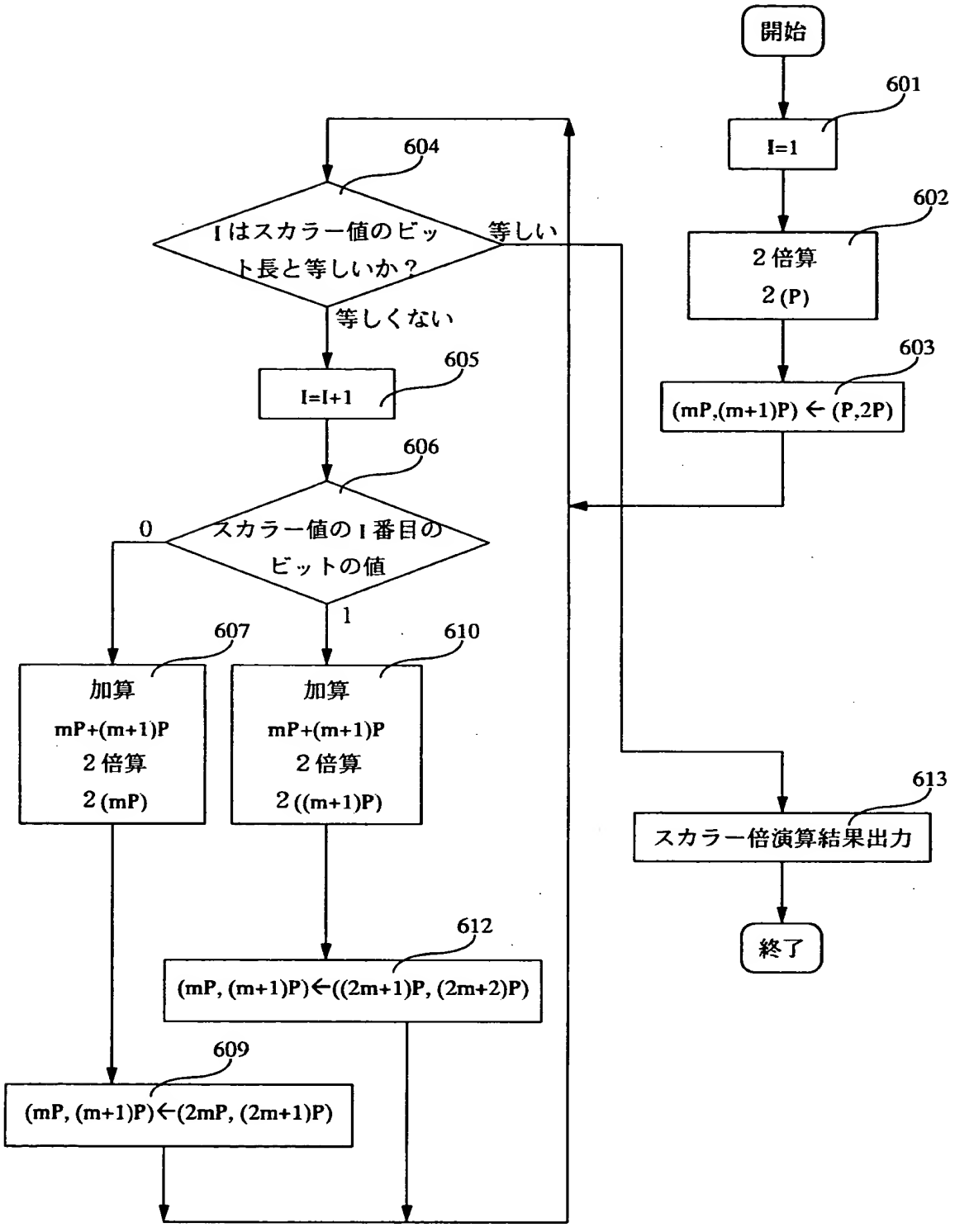
【図４】


開始
401
I=1
402
２倍算
２(P)
403
(mP,(m+1)P) ← (P,2P)
404
Iはスカラー値のビット長と等しいか？
等しい
等しくない
405
I=I+1
406
スカラー値のI番目のビットの値
0
1
407
２倍算
２(mP)
410
２倍算
２((m+1)P)
408
加算
mP+(m+1)P
411
加算
mP+(m+1)P
412
(mP, (m+1)P)←((2m+1)P, (2m+2)P)
409
(mP, (m+1)P)←(2mP, (2m+1)P)
413
スカラー倍演算結果出力
終了

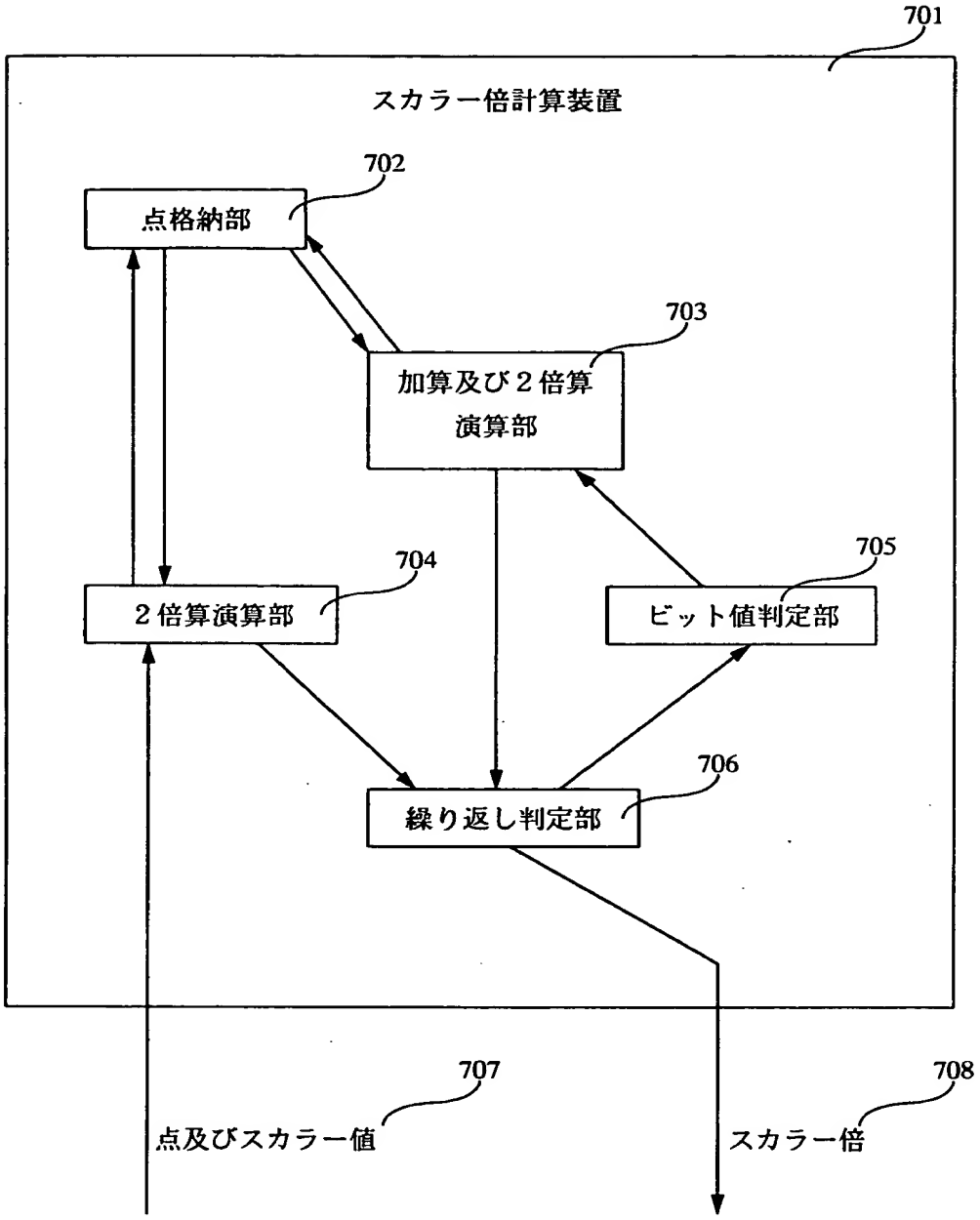
【図５】


501
スカラー倍計算装置
502
点格納部
503
加算演算部
504
２倍算演算部
505
ビット値判定部
506
繰り返し判定部
507
点及びスカラー値
508
スカラー倍

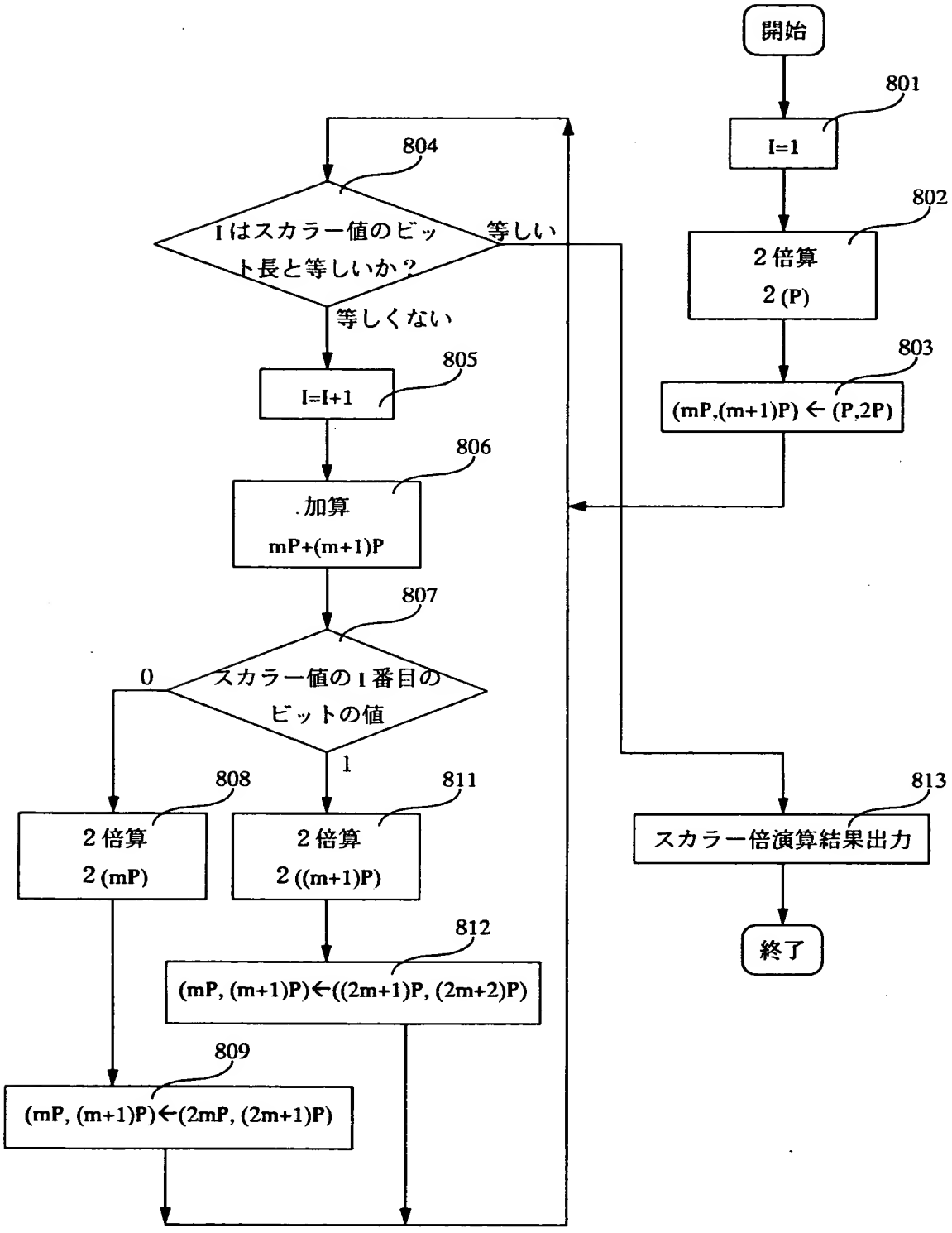
【図６】


開始
601
I=1
602
２倍算
２(P)
603
(mP,(m+1)P) ← (P,2P)
604
Iはスカラー値のビット長と等しいか？
等しい
等しくない
605
I=I+1
606
スカラー値のI番目のビットの値
0
1
607
加算
mP+(m+1)P
２倍算
２(mP)
610
加算
mP+(m+1)P
２倍算
２((m+1)P)
612
(mP, (m+1)P)←((2m+1)P, (2m+2)P)
609
(mP, (m+1)P)←(2mP, (2m+1)P)
613
スカラー倍演算結果出力
終了

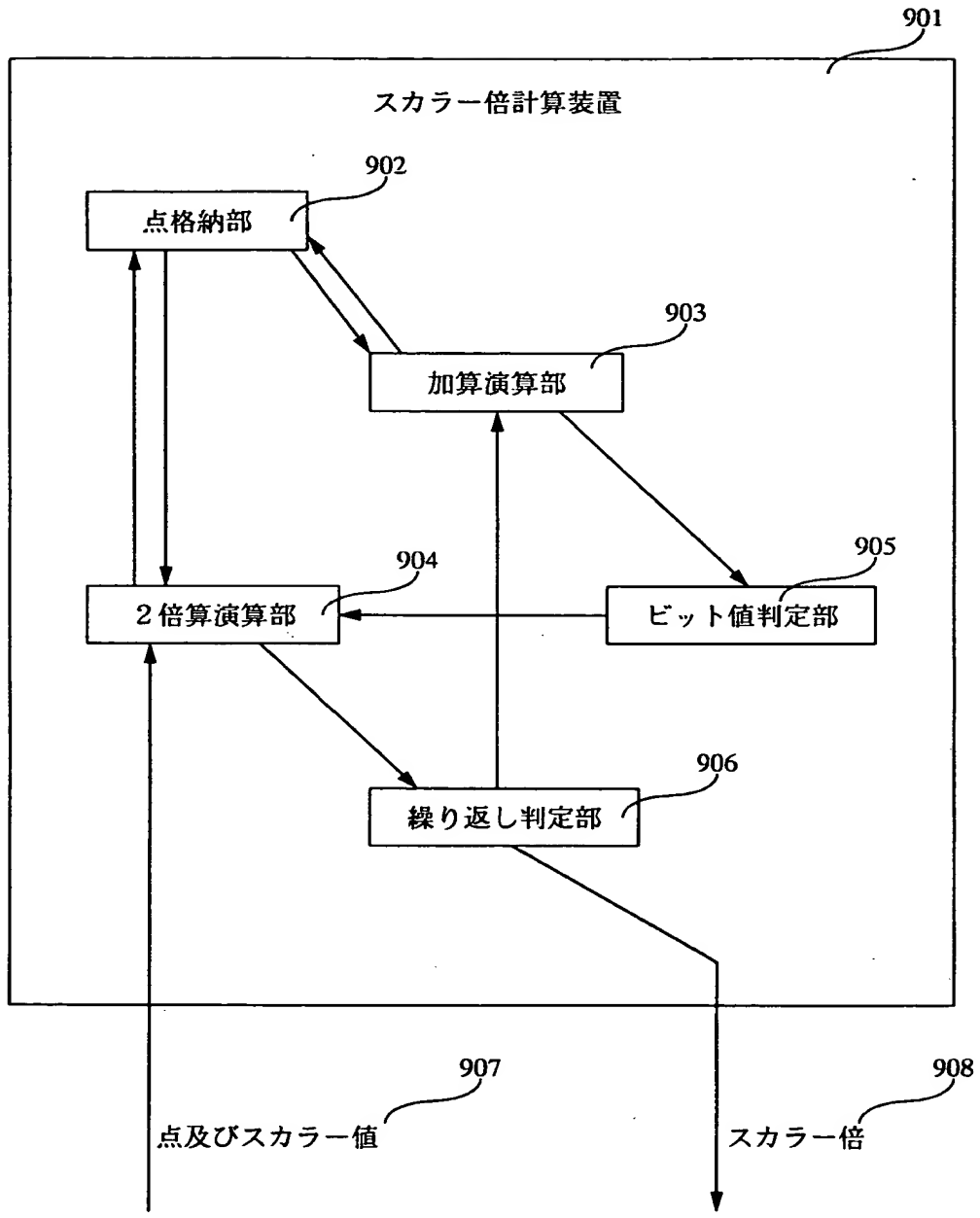
【図７】


701
スカラー倍計算装置
702
点格納部
703
加算及び２倍算
演算部
704
２倍算演算部
705
ビット値判定部
706
繰り返し判定部
707
点及びスカラー値
708
スカラー倍

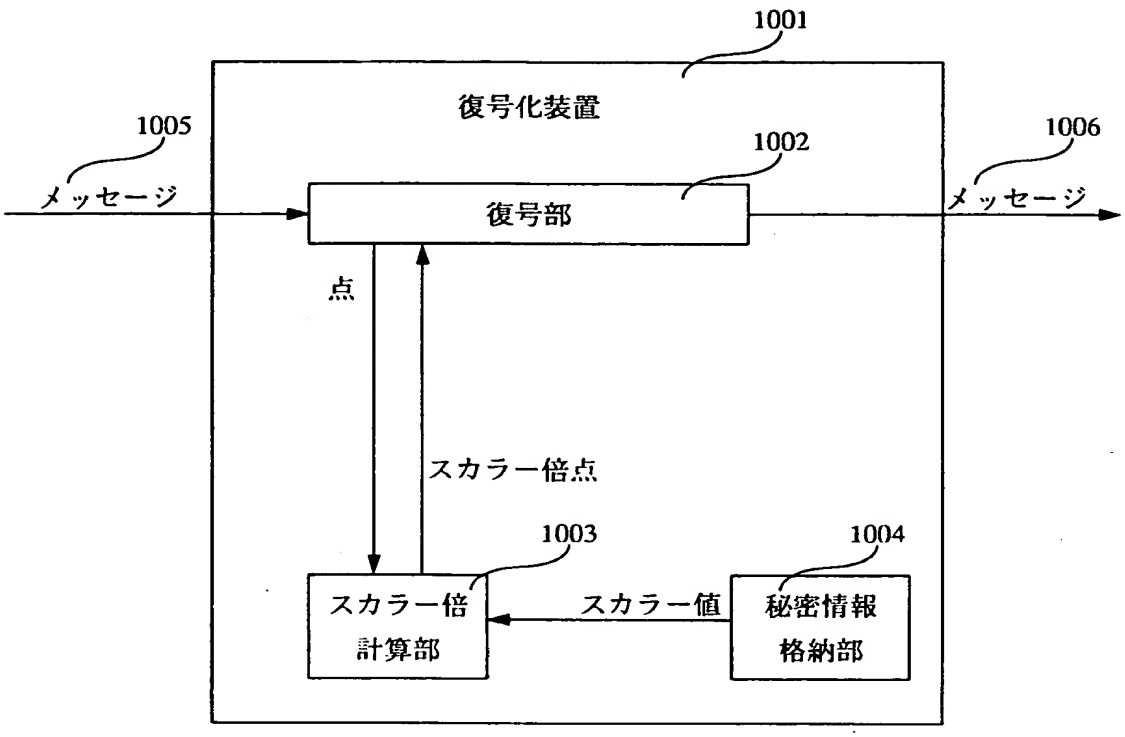
【図８】


開始
801
I=1
802
２倍算
２(P)
803
(mP,(m+1)P) ← (P,2P)
804
Iはスカラー値のビット長と等しいか？
等しい
等しくない
805
I=I+1
806
加算
mP+(m+1)P
807
スカラー値のI番目のビットの値
0
1
808
２倍算
２(mP)
811
２倍算
２((m+1)P)
812
(mP, (m+1)P)←((2m+1)P, (2m+2)P)
809
(mP, (m+1)P)←(2mP, (2m+1)P)
813
スカラー倍演算結果出力
終了

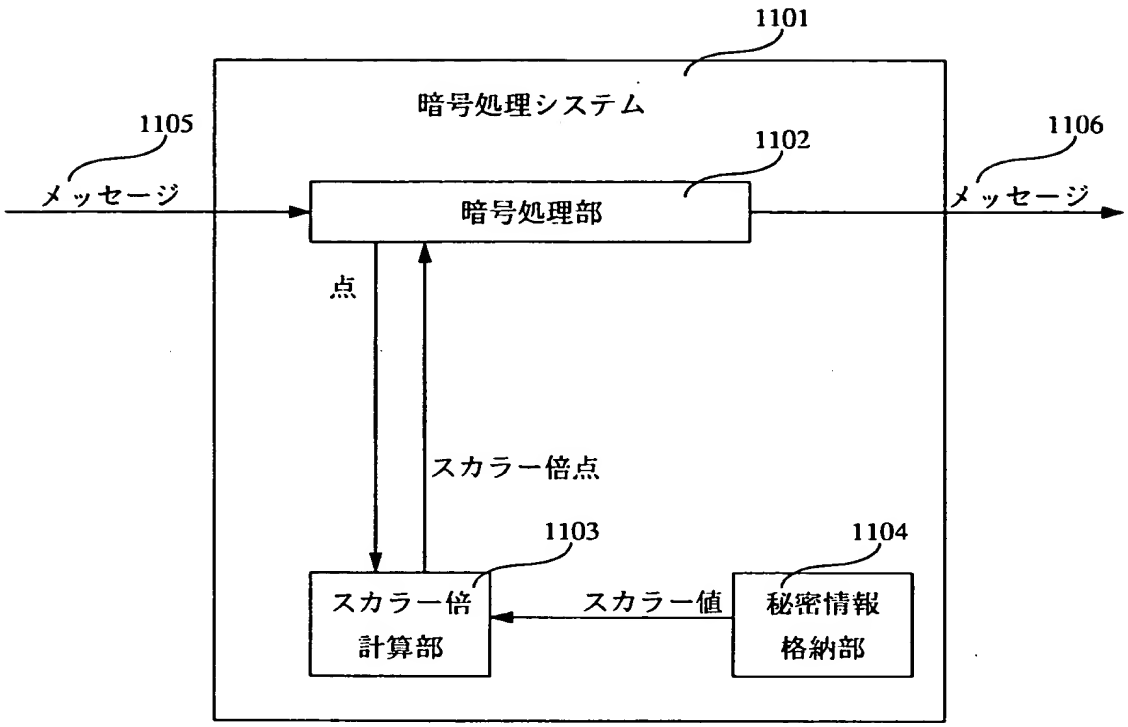
【図９】


901
スカラー倍計算装置
902
点格納部
903
加算演算部
904
２倍算演算部
905
ビット値判定部
906
繰り返し判定部
907
点及びスカラー値
908
スカラー倍

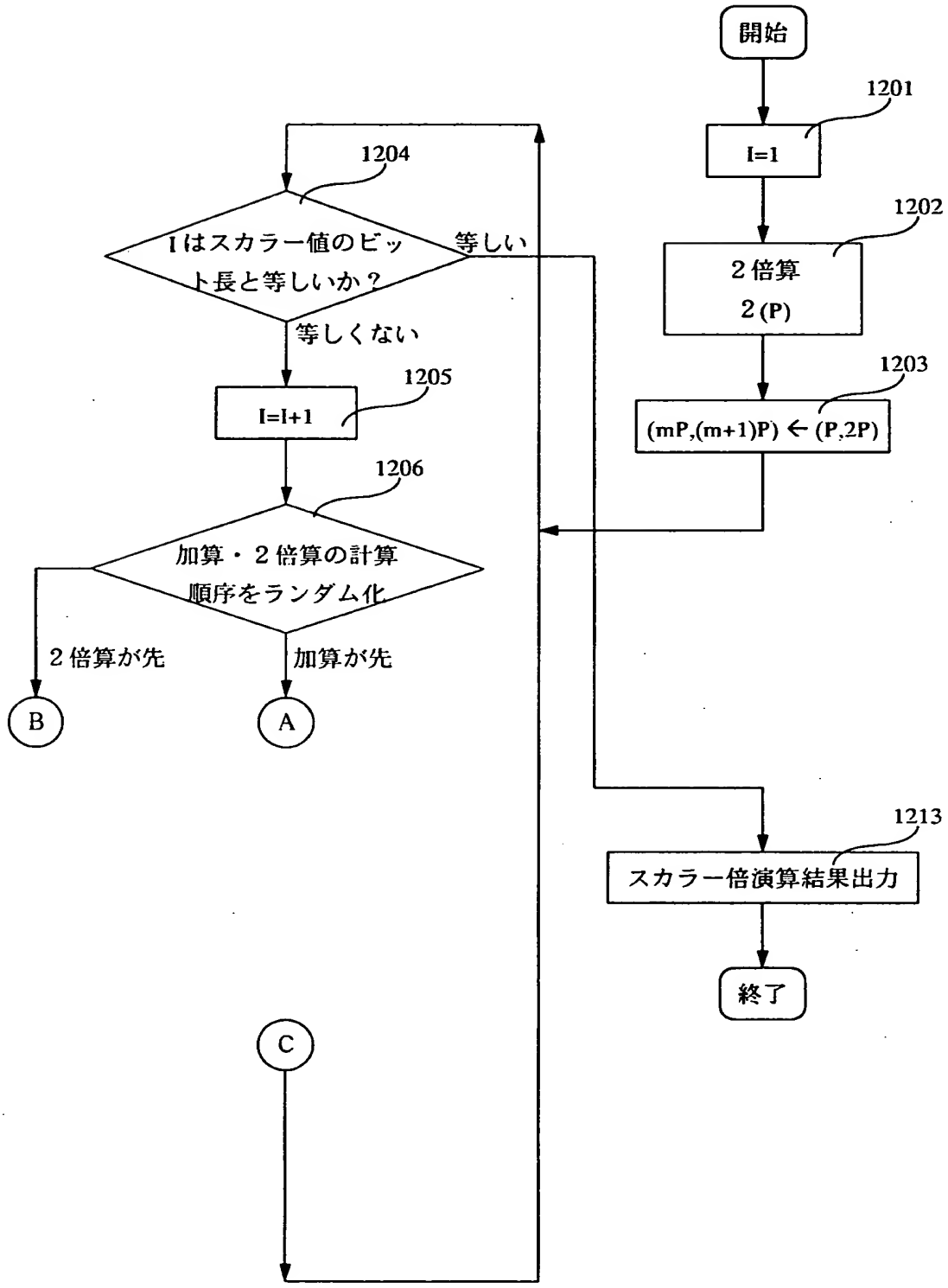
【図１０】


1001
復号化装置
1005
メッセージ
1002
復号部
1006
メッセージ
点
スカラー倍点
1003
1004
スカラー倍
計算部
スカラー値
秘密情報
格納部

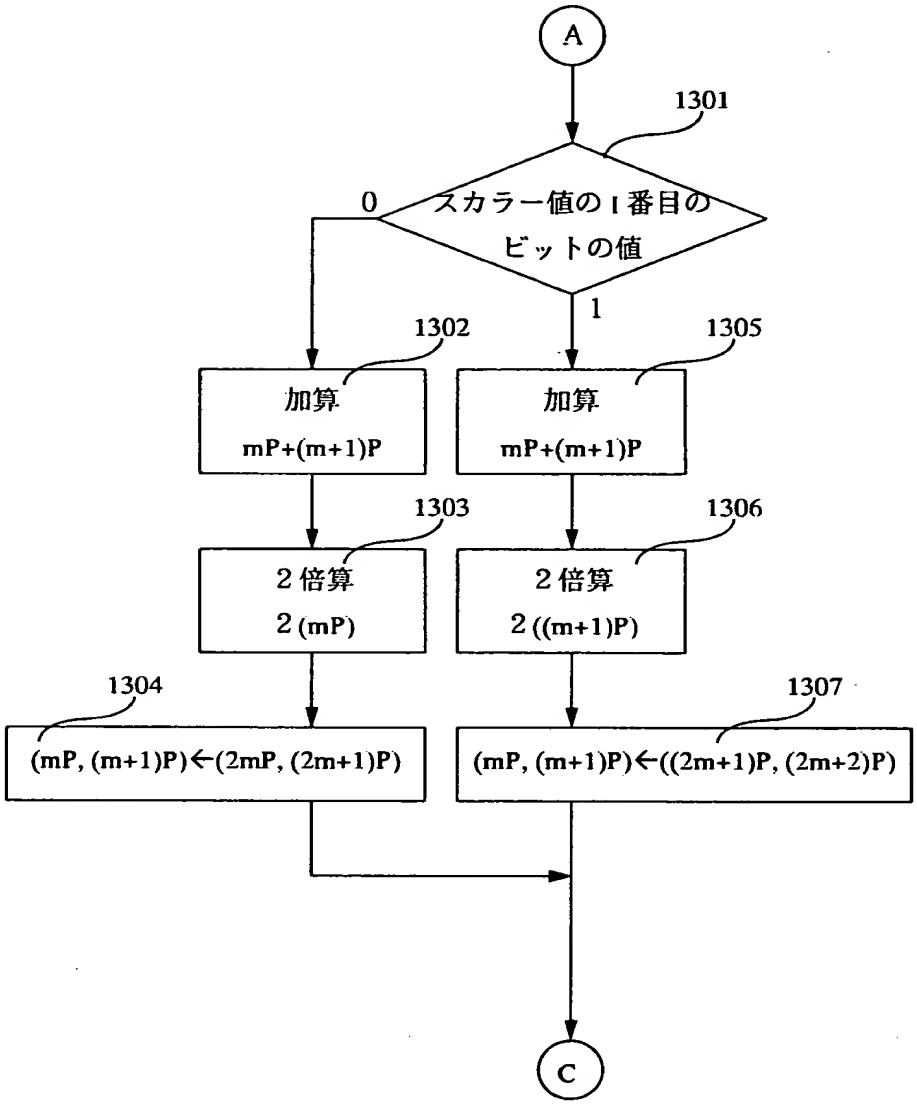
【図１１】


1101
暗号処理システム
1105
メッセージ
1102
暗号処理部
1106
メッセージ
点
スカラー倍点
1103
1104
スカラー倍
計算部
スカラー値
秘密情報
格納部

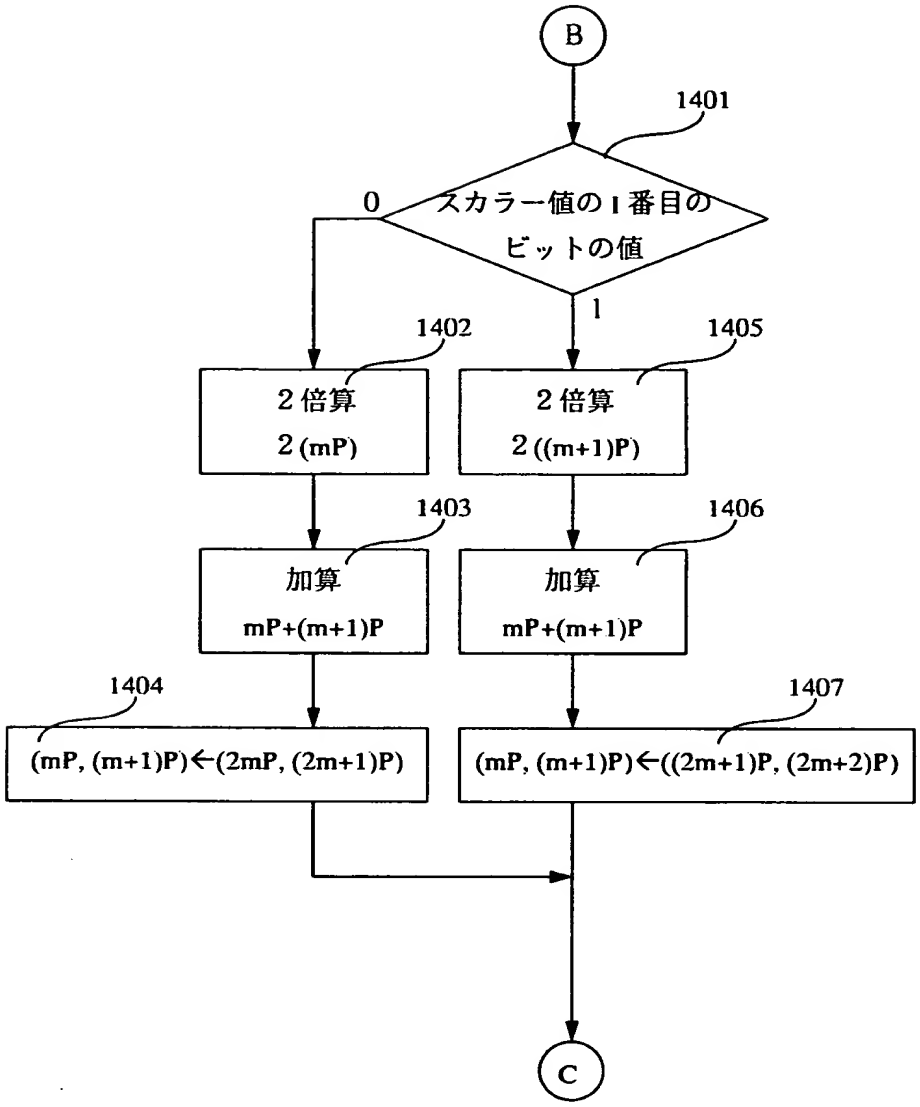
【図１２】


開始
1201
I=1
1202
２倍算
2(P)
1203
(mP,(m+1)P) ← (P,2P)
1204
Iはスカラー値のビット長と等しいか？
等しい
等しくない
1205
I=I+1
1206
加算・２倍算の計算順序をランダム化
２倍算が先
加算が先
B
A
C
1213
スカラー倍演算結果出力
終了

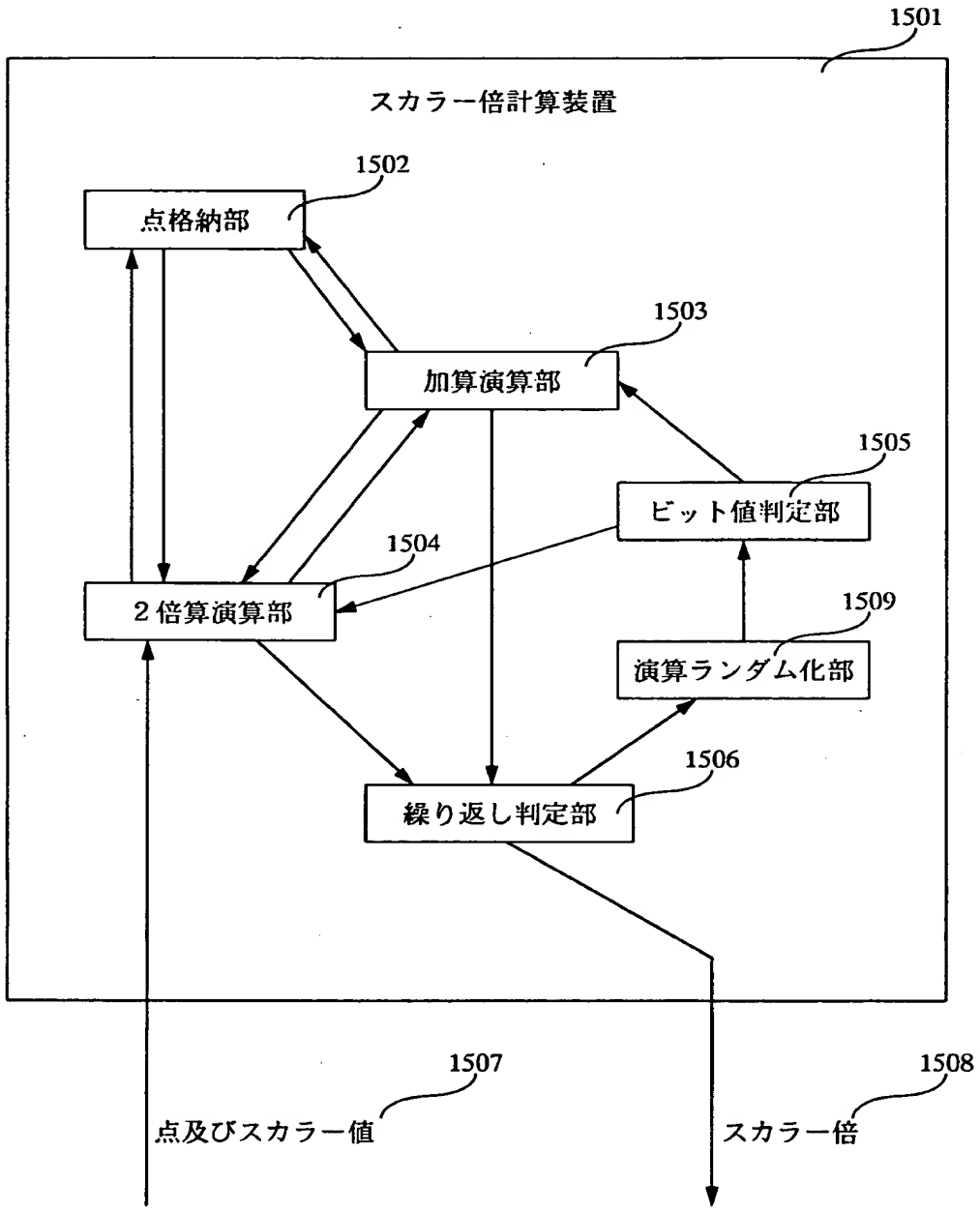
【図１３】


A
1301
スカラー値のi番目のビットの値
0
1
1302
加算
mP+(m+1)P
1305
加算
mP+(m+1)P
1303
2倍算
2(mP)
1306
2倍算
2((m+1)P)
1304
(mP, (m+1)P)←(2mP, (2m+1)P)
1307
(mP, (m+1)P)←((2m+1)P, (2m+2)P)
C

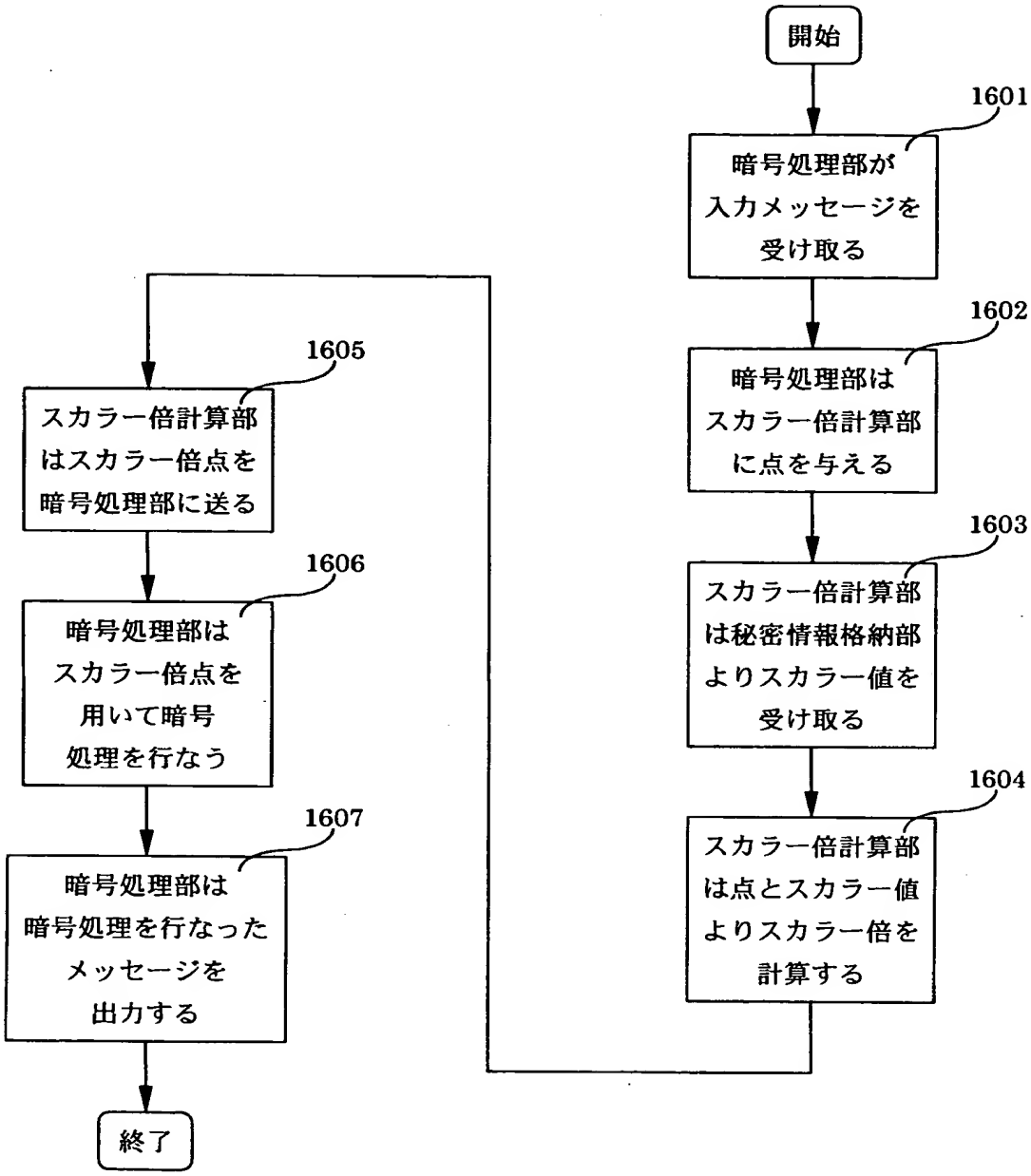
【図１４】


B
1401
スカラー値のｉ番目の
ビットの値
0
1
1402
２倍算
２(mP)
1405
２倍算
２((m+1)P)
1403
加算
mP+(m+1)P
1406
加算
mP+(m+1)P
1404
(mP, (m+1)P)←(2mP, (2m+1)P)
1407
(mP, (m+1)P)←((2m+1)P, (2m+2)P)
C

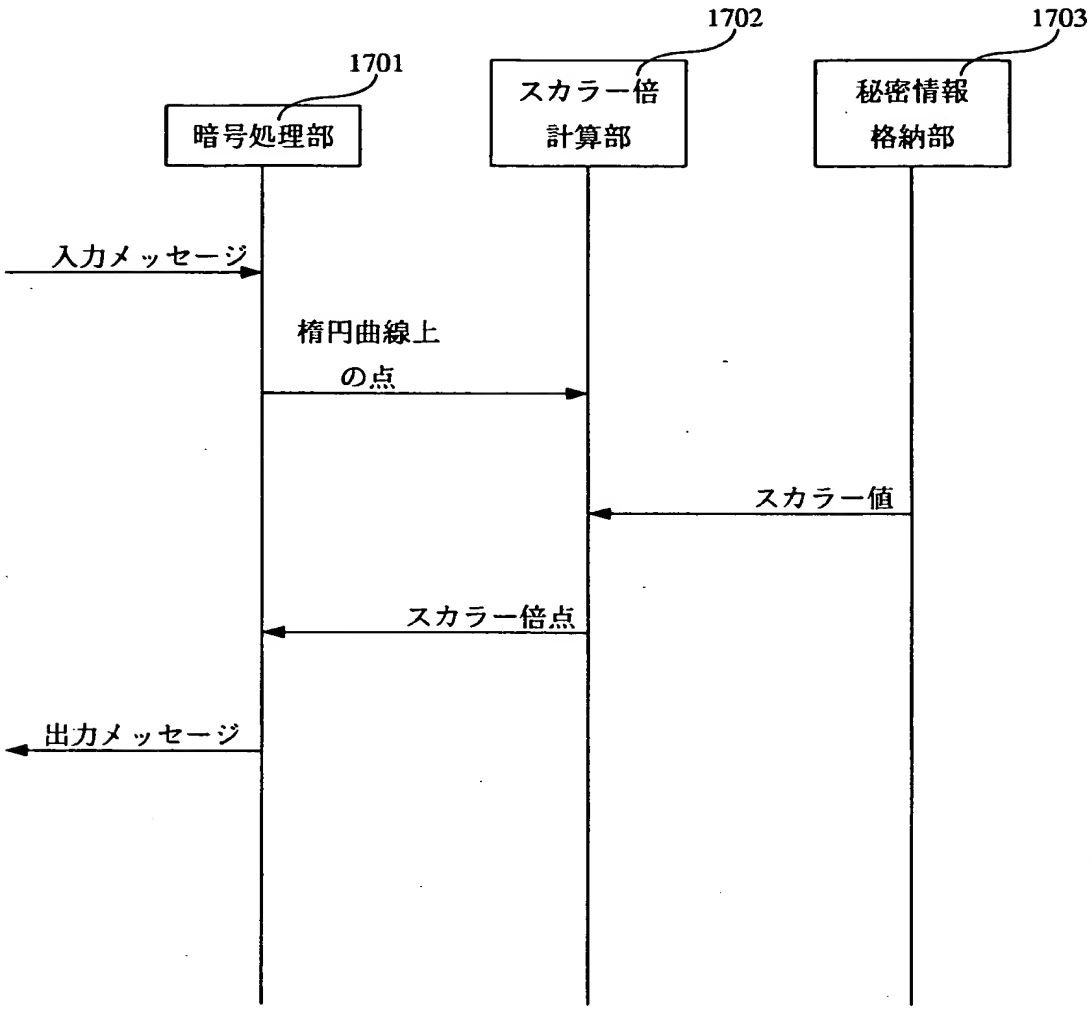
【図１５】


1501
スカラー倍計算装置
1502
点格納部
1503
加算演算部
1505
ビット値判定部
1504
２倍算演算部
1509
演算ランダム化部
1506
繰り返し判定部
1507
点及びスカラー値
1508
スカラー倍

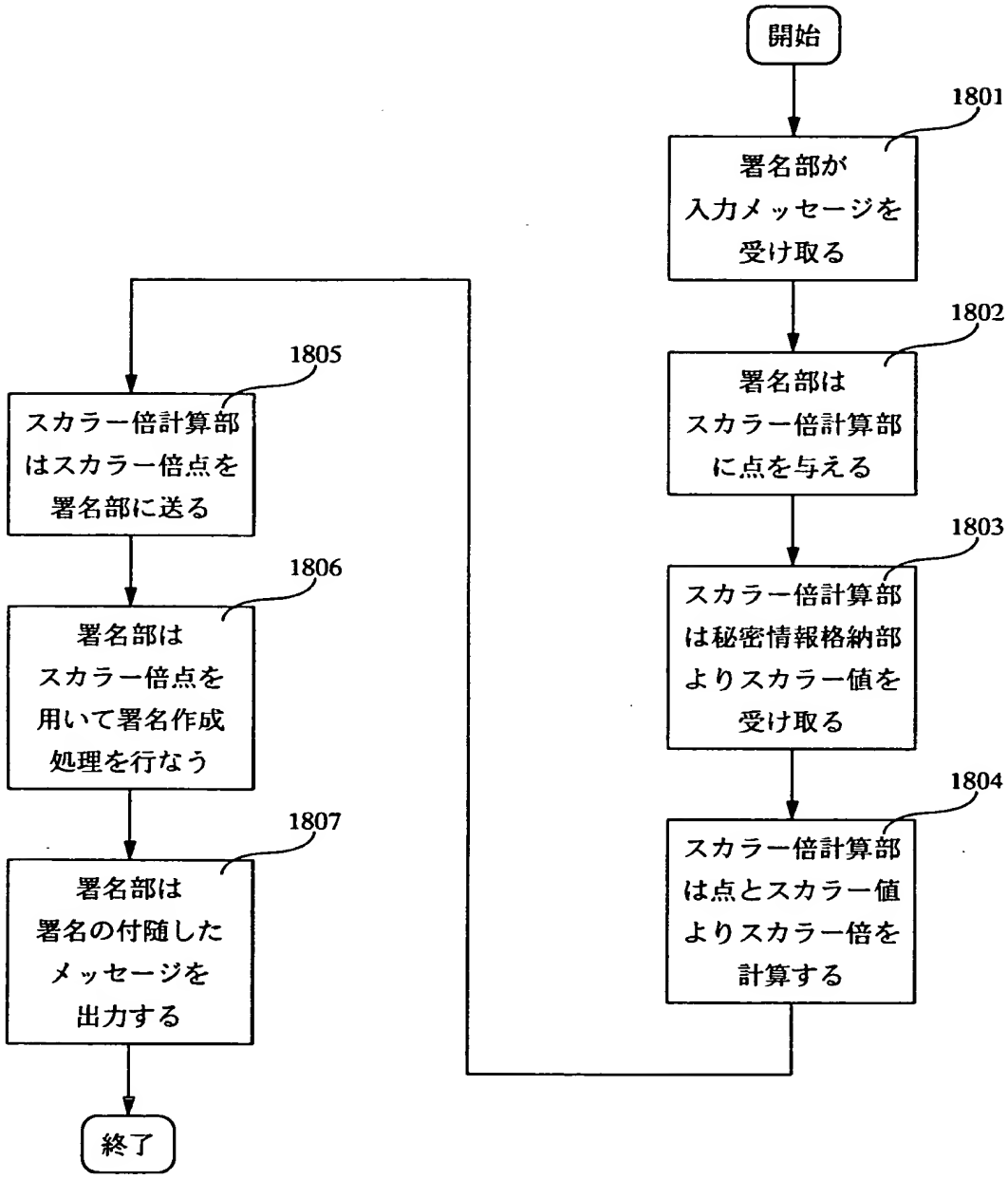
【図１６】


開始
1601
暗号処理部が
入力メッセージを
受け取る
1602
暗号処理部は
スカラー倍計算部
に点を与える
1603
スカラー倍計算部
は秘密情報格納部
よりスカラー値を
受け取る
1604
スカラー倍計算部
は点とスカラー値
よりスカラー倍を
計算する
1605
スカラー倍計算部
はスカラー倍点を
暗号処理部に送る
1606
暗号処理部は
スカラー倍点を
用いて暗号
処理を行なう
1607
暗号処理部は
暗号処理を行なった
メッセージを
出力する
終了

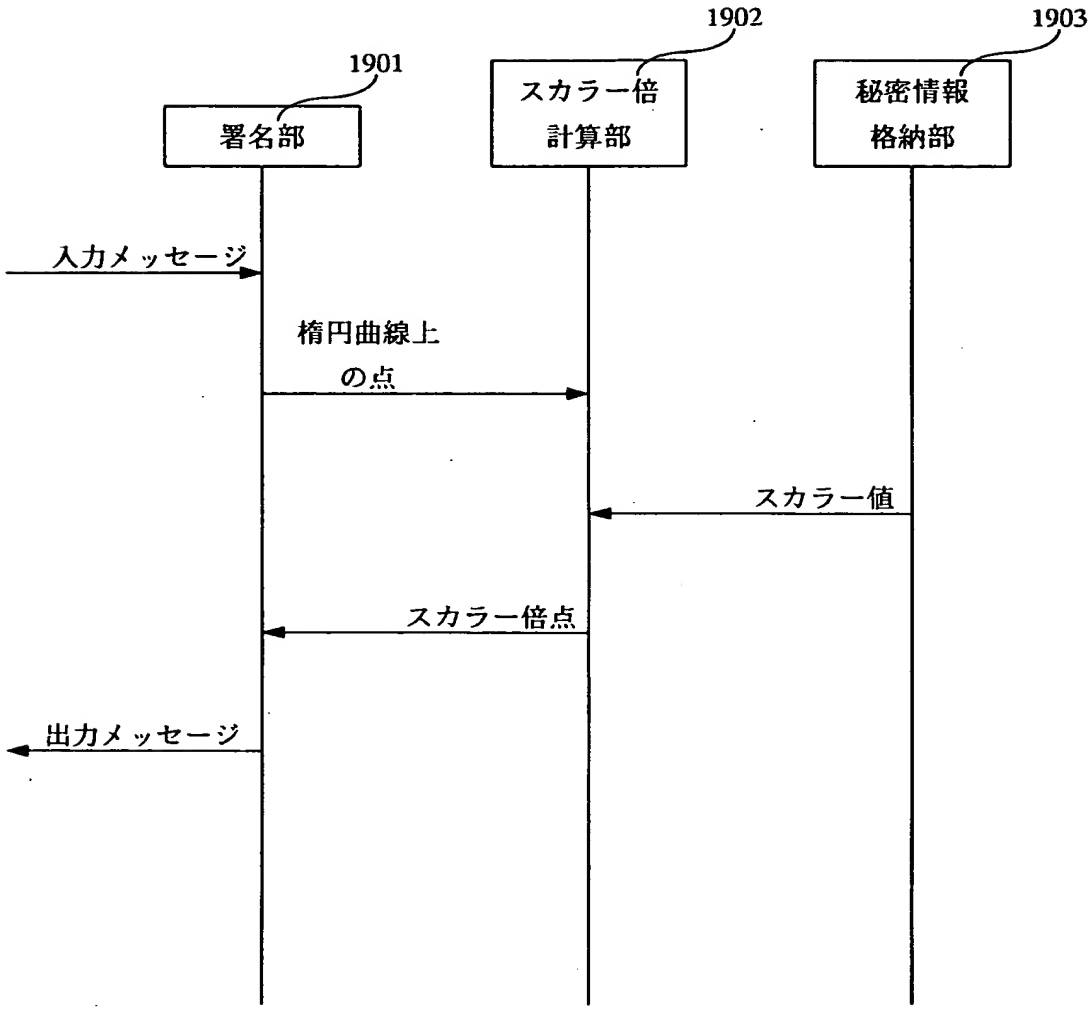
【図１７】


1701
暗号処理部
1702
スカラー倍
計算部
1703
秘密情報
格納部
入力メッセージ
楕円曲線上
の点
スカラー値
スカラー倍点
出力メッセージ

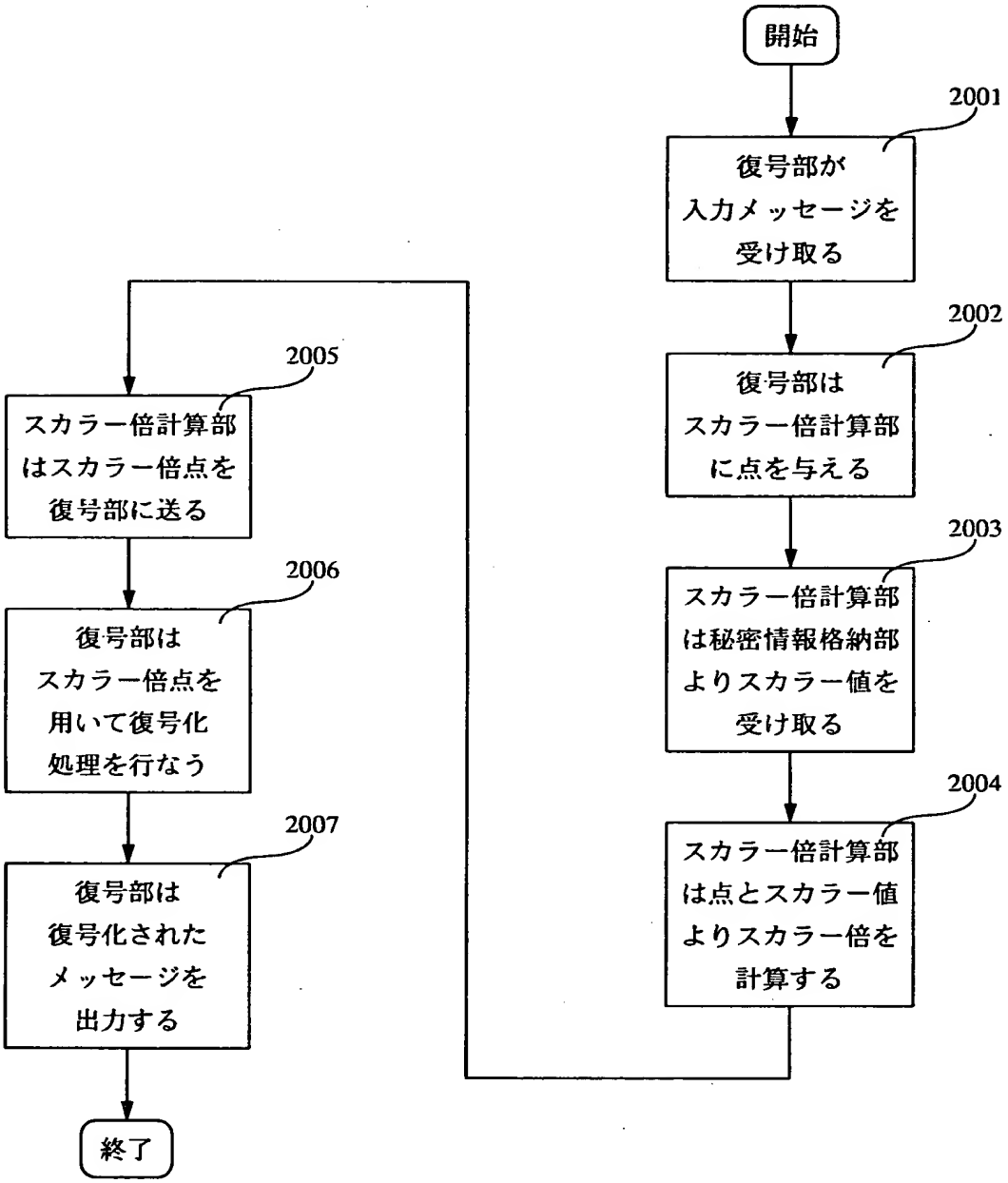
【図１８】


開始
1801
署名部が
入力メッセージを
受け取る
1802
署名部は
スカラー倍計算部
に点を与える
1803
スカラー倍計算部
は秘密情報格納部
よりスカラー値を
受け取る
1804
スカラー倍計算部
は点とスカラー値
よりスカラー倍を
計算する
1805
スカラー倍計算部
はスカラー倍点を
署名部に送る
1806
署名部は
スカラー倍点を
用いて署名作成
処理を行なう
1807
署名部は
署名の付随した
メッセージを
出力する
終了

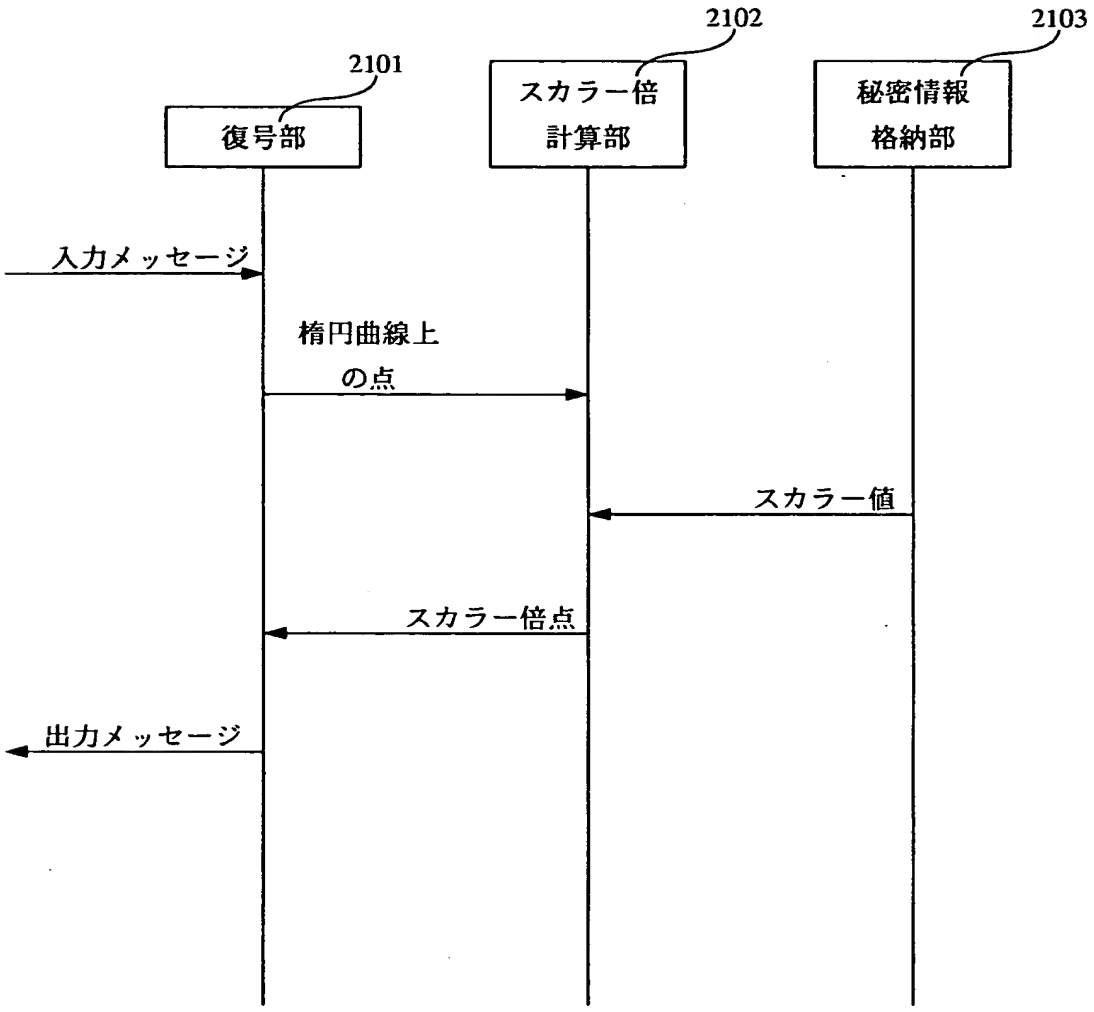
【図１９】


1901
署名部
1902
スカラー倍
計算部
1903
秘密情報
格納部
入力メッセージ
楕円曲線上
の点
スカラー値
スカラー倍点
出力メッセージ

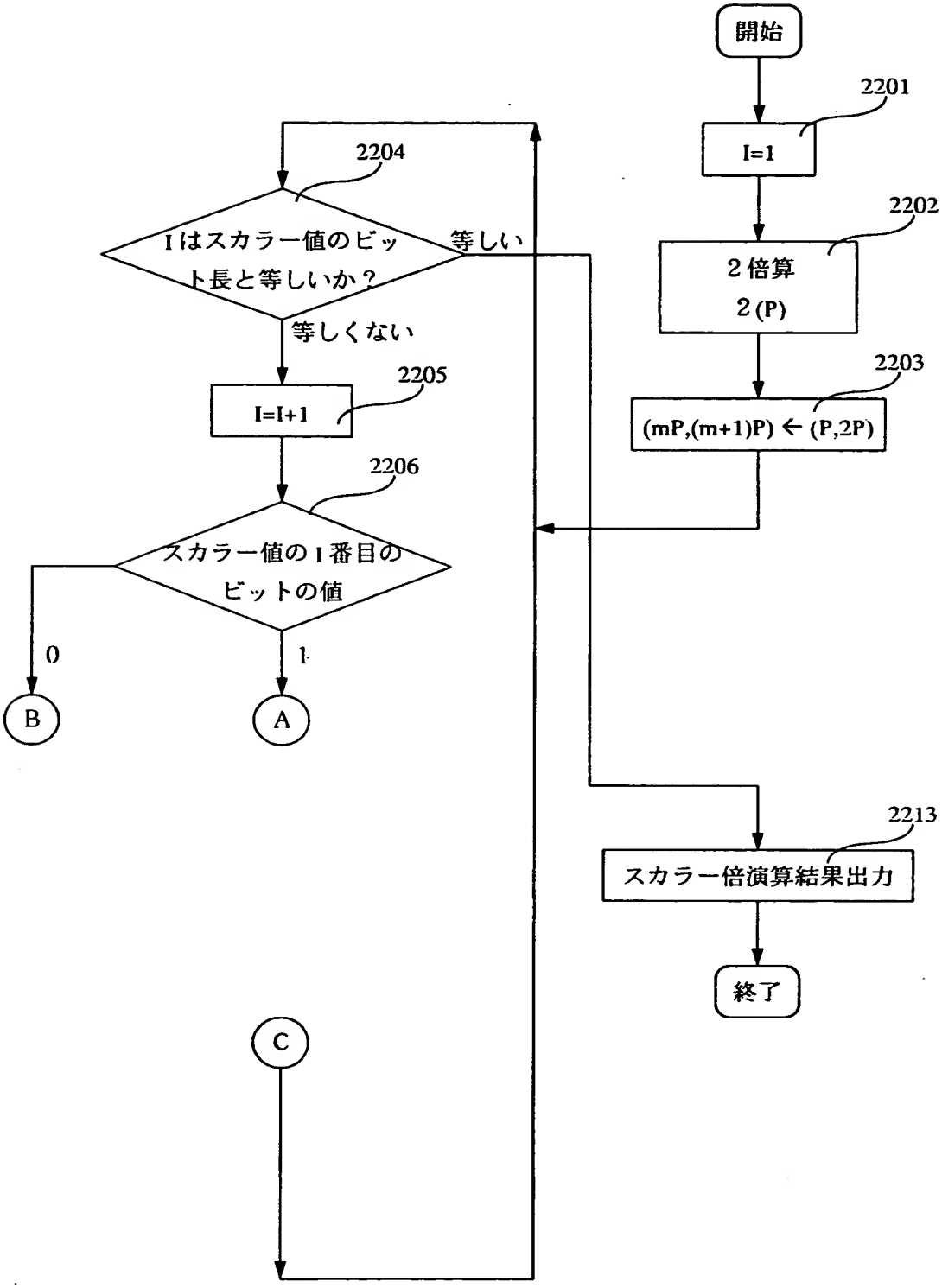
【図２０】


開始
2001
復号部が
入力メッセージを
受け取る
2002
復号部は
スカラー倍計算部
に点を与える
2003
スカラー倍計算部
は秘密情報格納部
よりスカラー値を
受け取る
2004
スカラー倍計算部
は点とスカラー値
よりスカラー倍を
計算する
2005
スカラー倍計算部
はスカラー倍点を
復号部に送る
2006
復号部は
スカラー倍点を
用いて復号化
処理を行なう
2007
復号部は
復号化された
メッセージを
出力する
終了

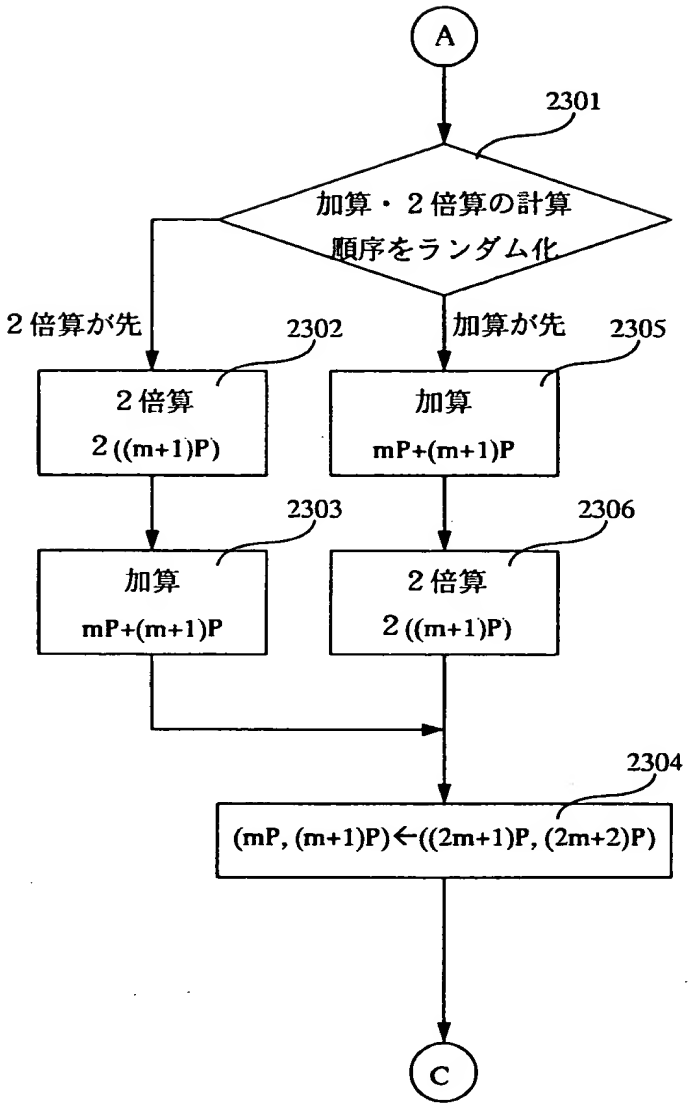
【図２１】


2101
復号部
2102
スカラー倍
計算部
2103
秘密情報
格納部
入力メッセージ
楕円曲線上
の点
スカラー値
スカラー倍点
出力メッセージ

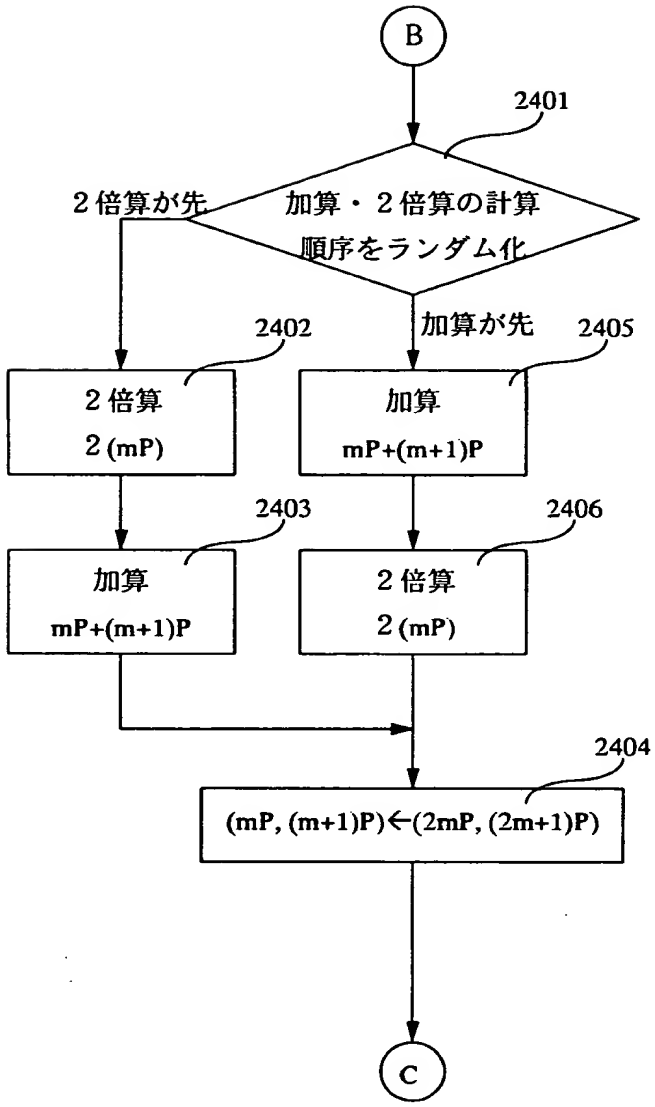
【図２２】


開始
2201
I=1
2202
２倍算
２(P)
2203
(mP,(m+1)P) ← (P,2P)
2204
Iはスカラー値のビット長と等しいか？
等しい
等しくない
2205
I=I+1
2206
スカラー値のI番目のビットの値
0
1
B
A
C
2213
スカラー倍演算結果出力
終了

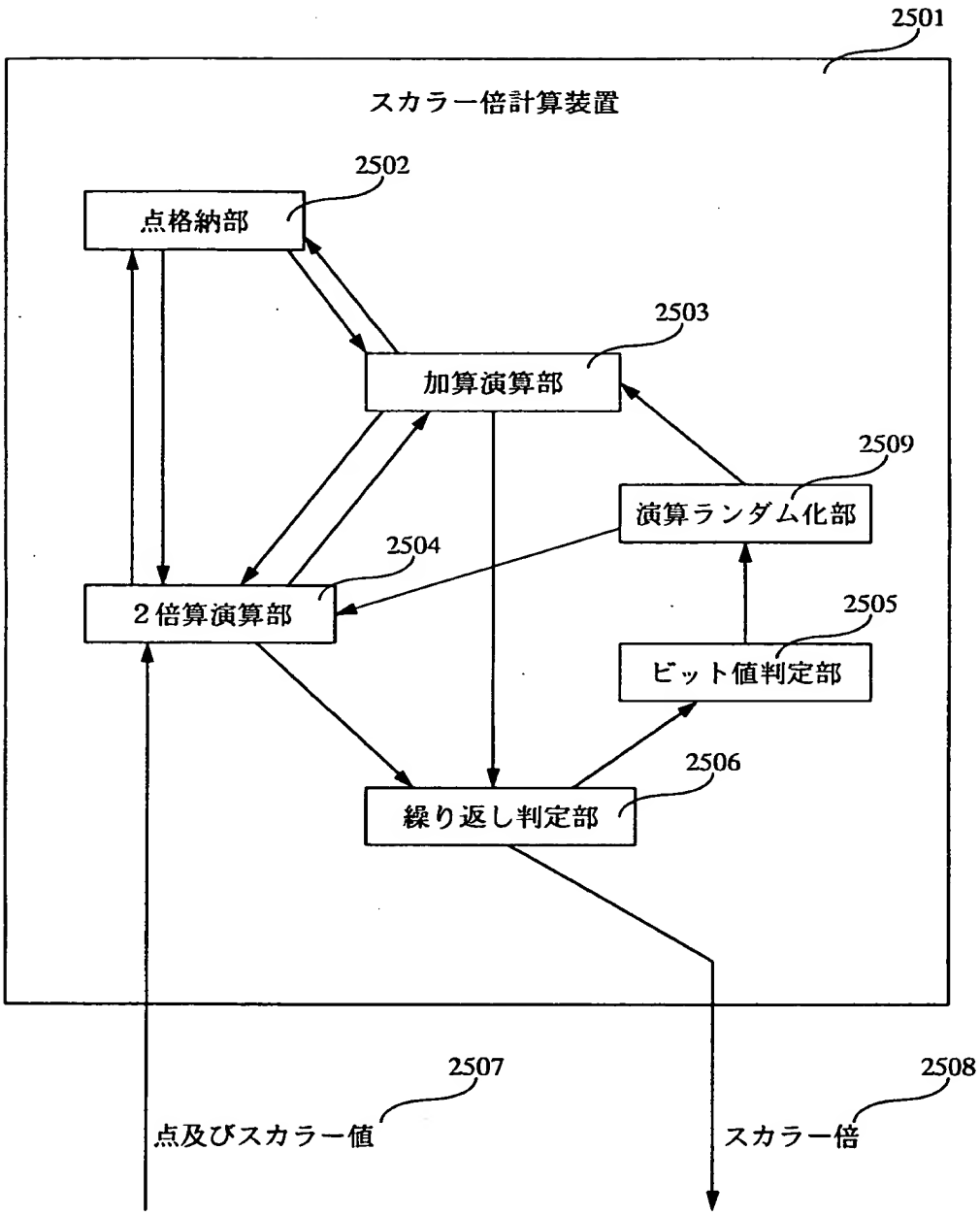
【図２３】


A
2301
加算・２倍算の計算
順序をランダム化
２倍算が先
加算が先
2302
2305
２倍算
2((m+1)P)
加算
mP+(m+1)P
2303
2306
加算
mP+(m+1)P
２倍算
2((m+1)P)
2304
(mP, (m+1)P)←((2m+1)P, (2m+2)P)
C

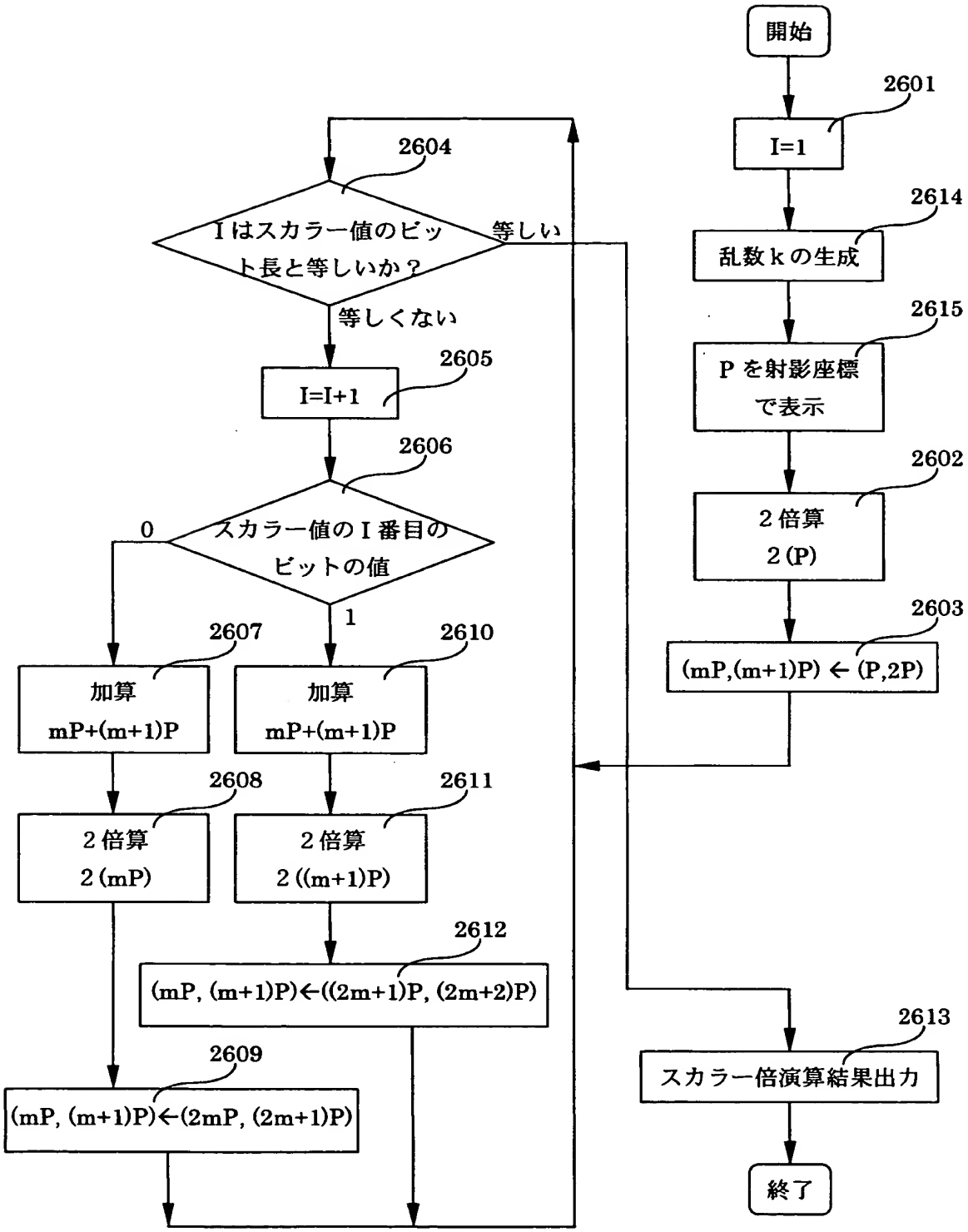
【図２４】


B
2401
加算・２倍算の計算順序をランダム化
２倍算が先
加算が先
2402
２倍算
2(mP)
2405
加算
mP+(m+1)P
2403
加算
mP+(m+1)P
2406
２倍算
2(mP)
2404
(mP, (m+1)P)←(2mP, (2m+1)P)
C

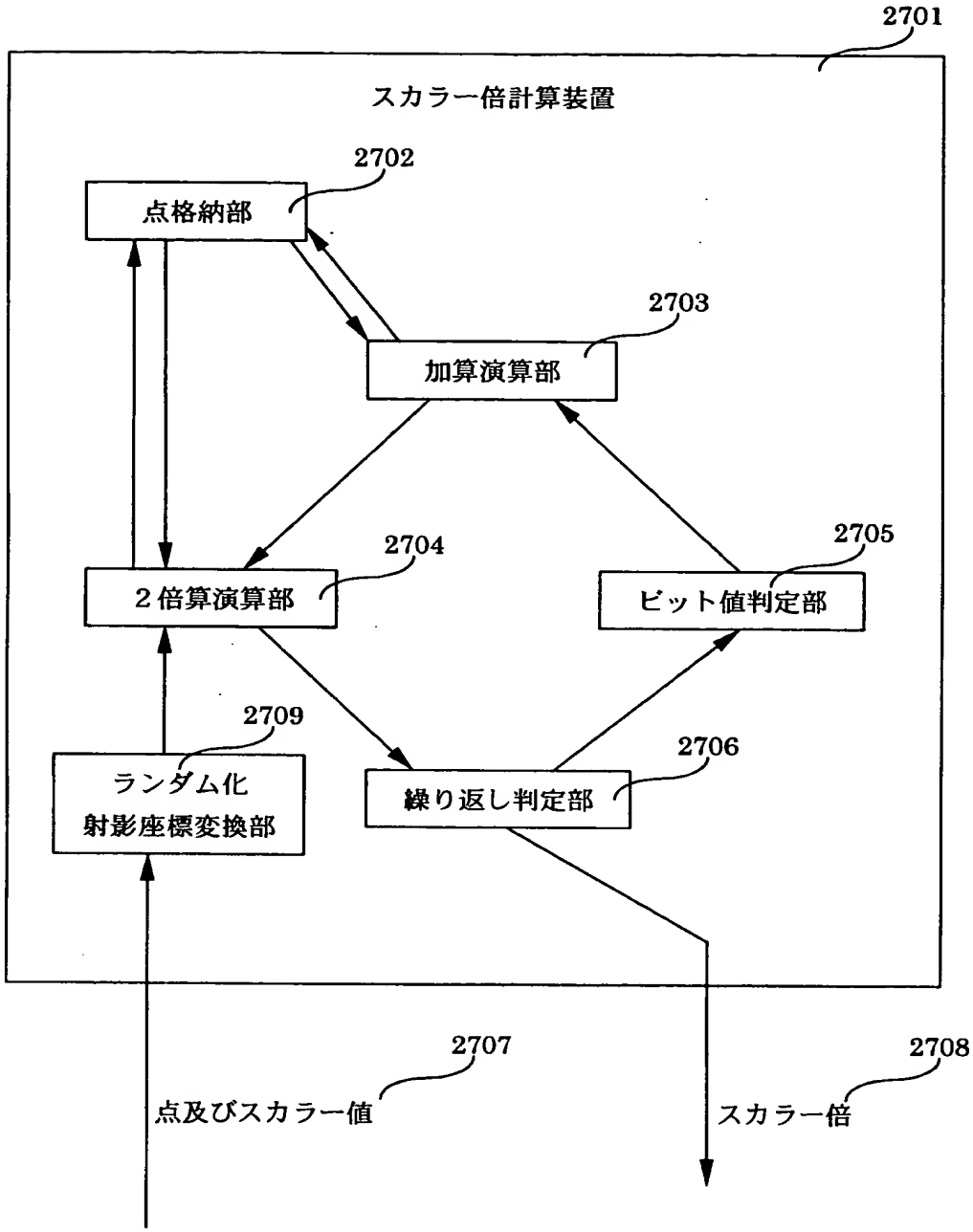
【図２５】


2501
スカラー倍計算装置
2502
点格納部
2503
加算演算部
2509
演算ランダム化部
2504
２倍算演算部
2505
ビット値判定部
2506
繰り返し判定部
2507
点及びスカラー値
2508
スカラー倍

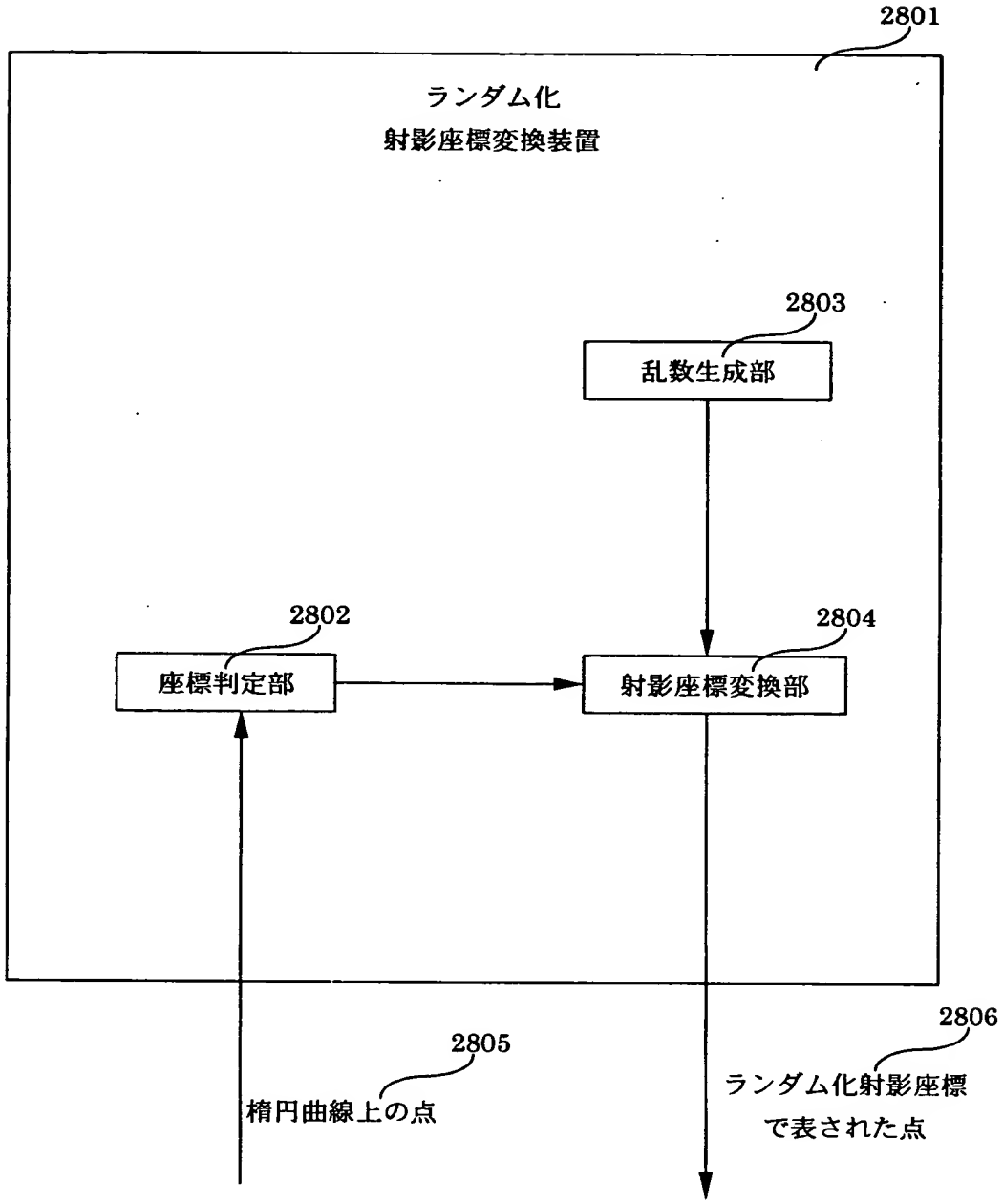
【図２６】


開始
2601
I=1
2614
乱数ｋの生成
2615
Ｐを射影座標で表示
2602
２倍算 2(P)
2603
(mP,(m+1)P) ← (P,2P)
2604
Ｉはスカラー値のビット長と等しいか？
等しい
等しくない
2605
I=I+1
2606
スカラー値のＩ番目のビットの値
0
1
2607
加算 mP+(m+1)P
2610
加算 mP+(m+1)P
2608
２倍算 2(mP)
2611
２倍算 2((m+1)P)
2612
(mP, (m+1)P)←((2m+1)P, (2m+2)P)
2609
(mP, (m+1)P)←(2mP, (2m+1)P)
2613
スカラー倍演算結果出力
終了

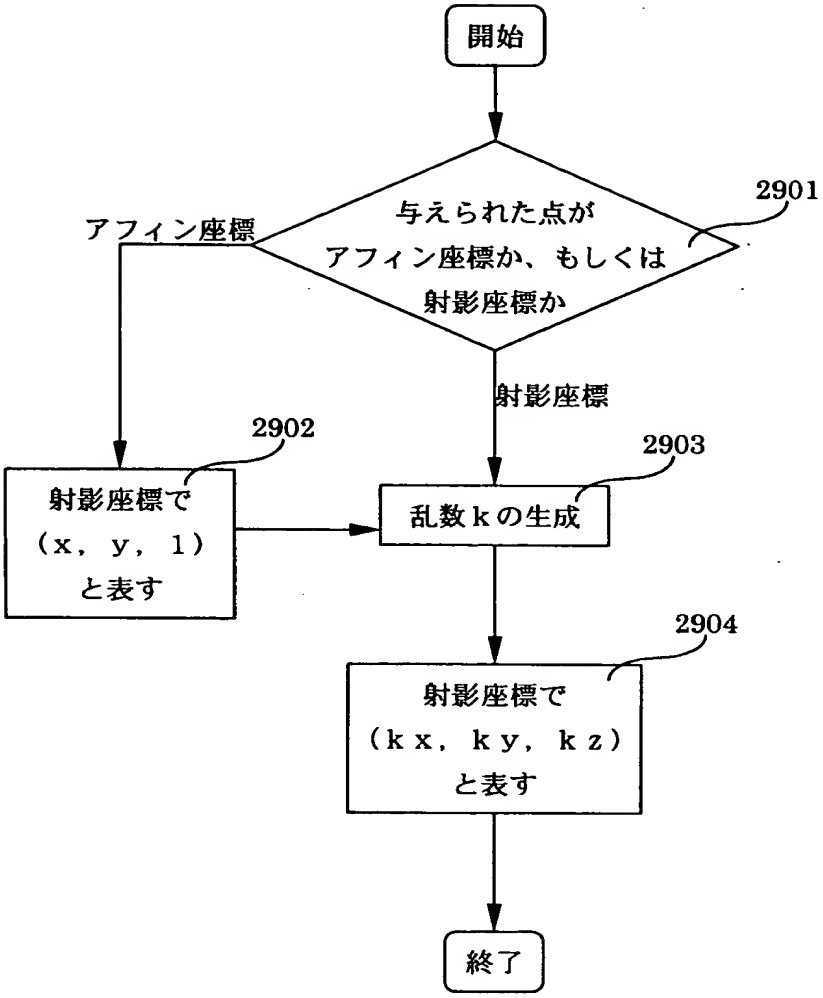
【図２７】


2701
スカラー倍計算装置
2702
点格納部
2703
加算演算部
2704
２倍算演算部
2705
ビット値判定部
2709
ランダム化
射影座標変換部
2706
繰り返し判定部
2707
点及びスカラー値
2708
スカラー倍

【図２８】


2801
ランダム化
射影座標変換装置
2803
乱数生成部
2802
座標判定部
2804
射影座標変換部
2805
楕円曲線上の点
2806
ランダム化射影座標
で表された点

【図２９】


開始
与えられた点が
アフィン座標か、もしくは
射影座標か
2901
アフィン座標
射影座標
2902
射影座標で
（x，y，1）
と表す
2903
乱数ｋの生成
2904
射影座標で
（ｋｘ，ｋｙ，ｋｚ）
と表す
終了

【書類名】　要約書

【要約】

【課題】

楕円曲線暗号における秘密情報を用いた暗号処理において、ＤＰＡ等のパワーアナリシスという攻撃法により、暗号処理経過から秘密情報が復元される可能性があった。本発明の目的は、パワーアナリシスにより暗号処理経過が漏洩しても、秘密情報自体は漏洩せず、しかも高速に暗号処理を実行できる暗号処理方法を提供することにある。

【解決手段】

暗号処理経過と秘密情報との依存関係を断ち切った暗号処理方法を与える。特に、秘密情報であるスカラー値に対して、スカラー倍計算経過がそれらの値に依存しないスカラー倍計算方法を与える。すなわち、楕円曲線暗号においてスカラー値及び楕円曲線上の点からスカラー倍点を計算する際、スカラー値のビットの値を判定し、その判定を行なったビットの値に依存せずに一定の回数及び一定の順序で楕円曲線上の演算を実行する。

【選択図】　図２

認定・付加情報

特許出願の番号	特願２０００－１６０００１
受付番号	５００００６６７１４１
書類名	特許願
担当官	第七担当上席　　００９６
作成日	平成１２年　５月３１日

＜認定情報・付加情報＞

【提出日】　平成12年 5月30日

次頁無

出　願　人　履　歴　情　報

識別番号　　〔０００００５１０８〕

１．変更年月日　　１９９０年　８月３１日
［変更理由］　新規登録
住　所　東京都千代田区神田駿河台４丁目６番地
氏　名　株式会社日立製作所

く。

【００７０】

ステップ１３０２として、加算演算部１５０３により、点格納部１５０２に格納されている点の組（ｍＰ，（ｍ＋１）Ｐ）から点ｍＰと点（ｍ＋１）Ｐの加算ｍＰ＋（ｍ＋１）Ｐを行ない、点（２ｍ＋１）Ｐを計算する。その後ステップ１３０３へ行く。ステップ１３０３として、２倍算演算部１５０４により、点格納部１５０２に格納されている点の組（ｍＰ，（ｍ＋１）Ｐ）から点ｍＰの２倍算２（ｍＰ）を行ない、点２ｍＰを計算する。その後ステップ１３０４へ行く。ステップ１３０４として、ステップ１３０３で求めた点２ｍＰとステップ１３０２で求めた点（２ｍ＋１）Ｐを点格納部１５０２に点の組（２ｍＰ，（２ｍ＋１）Ｐ）として、点の組（ｍＰ，（ｍ＋１）Ｐ）の代わりに格納する。その後ステップ１２０４へ戻る。

【００７１】

ステップ１３０５として、加算演算部１５０３により、点格納部１５０２に格納されている点の組（ｍＰ，（ｍ＋１）Ｐ）から点ｍＰと点（ｍ＋１）Ｐの加算ｍＰ＋（ｍ＋１）Ｐを行ない、点（２ｍ＋１）Ｐを計算する。その後ステップ１３０６へ行く。ステップ１３０６として、２倍算演算部１５０４により、点格納部１５０２に格納されている点の組（ｍＰ，（ｍ＋１）Ｐ）から点（ｍ＋１）Ｐの２倍算２（（ｍ＋１）Ｐ）を行ない、点（２ｍ＋２）Ｐを計算する。その後ステップ１３０７へ行く。ステップ１３０７として、ステップ１３０５で求めた点（２ｍ＋１）Ｐとステップ１３０６で求めた点（２ｍ＋２）Ｐを点格納部１５０２に点の組（（２ｍ＋１）Ｐ，（２ｍ＋２）Ｐ）として、点の組（ｍＰ，（ｍ＋１）Ｐ）の代わりに格納する。その後ステップ１２０４へ戻る。

【００７２】

ステップ１４０１として、ビット値判定部１５０５により、スカラー値のＩ番目のビットの値が０であるか１であるかを判定する。そのビットの値が０であればステップ１４０２へ行く。そのビットの値が１であればステップ１４０５へ行く。

【００７３】

ステップ１４０２として、２倍算演算部１５０４により、点格納部１５０２に格納されている点の組（ｍＰ，（ｍ＋１）Ｐ）から点ｍＰの２倍算２（ｍＰ）を行ない、点２ｍＰを計算する。その後ステップ１４０３へ行く。ステップ１４０３として、加算演算部１５０３により、点格納部１５０２に格納されている点の組（ｍＰ，（ｍ＋１）Ｐ）から点ｍＰと点（ｍ＋１）Ｐの加算ｍＰ＋（ｍ＋１）Ｐを行ない、点（２ｍ＋１）Ｐを計算する。その後ステップ１４０４へ行く。ステップ１４０４として、ステップ１４０２で求めた点２ｍＰとステップ１４０３で求めた点（２ｍ＋１）Ｐを点格納部１５０２に点の組（２ｍＰ，（２ｍ＋１）Ｐ）として、点の組（ｍＰ，（ｍ＋１）Ｐ）の代わりに格納する。その後ステップ１２０４へ戻る。

【００７４】

ステップ１４０５として、２倍算演算部１５０４により、点格納部１５０２に格納されている点の組（ｍＰ，（ｍ＋１）Ｐ）から点（ｍ＋１）Ｐの２倍算２（（ｍ＋１）Ｐ）を行ない、点（２ｍ＋２）Ｐを計算する。その後ステップ１４０６へ行く。ステップ１４０６として、加算演算部１５０３により、点格納部１５０２に格納されている点の組（ｍＰ，（ｍ＋１）Ｐ）から点ｍＰと点（ｍ＋１）Ｐの加算ｍＰ＋（ｍ＋１）Ｐを行ない、点（２ｍ＋１）Ｐを計算する。その後ステップ１４０７へ行く。ステップ１４０７として、ステップ１４０６で求めた点（２ｍ＋１）Ｐとステップ１４０５で求めた点（２ｍ＋２）Ｐを点格納部１５０２に点の組（（２ｍ＋１）Ｐ，（２ｍ＋２）Ｐ）として、点の組（ｍＰ，（ｍ＋１）Ｐ）の代わりに格納する。その後ステップ１２０４へ戻る。

【００７５】

ステップ１２１３として、点格納部１５０２に格納されている点の組（ｍＰ，（ｍ＋１）Ｐ）から、点ｍＰをスカラー倍１５０８として出力し、終了する。

【００７６】

以上の手順により出力する値である点ｍＰが点Ｐのスカラー値ｄによるスカラー倍の点ｄＰとなることは、第１実施例の場合と同様に示すことができる。

【００７７】

また、楕円曲線としてモンゴメリ型楕円曲線を用いると、加算及び２倍算が高

速に実行可能であり、通常用いる標準型楕円曲線よりも高速にスカラー倍計算が実行可能である。

【００７８】

標数２の有限体上で定義された楕円曲線に対しても、上記手順において加算及び２倍算の計算に高速な加算及び２倍算の計算方法を用いることにより、標数２の有限体上で定義された楕円曲線の通常のスカラー倍計算と比べて、高速にスカラー倍計算が実行可能である。

【００７９】

図２５は、図１１の暗号処理システム１１０１における秘密情報を用いた暗号処理において、暗号処理経過が漏洩しても秘密情報は漏洩しないスカラー倍計算方法の第６実施例を示す図である。図２２、図２３及び図２４は、第６実施例のスカラー倍計算方法を示すフローチャートである。図２２～図２５を参照して、第６実施例を説明する。

【００８０】

スカラー倍計算装置２５０１では、点及びスカラー値２５０７を入力し、以下の手順でスカラー倍２５０８を出力する。ステップ２２０１として、繰り返し判定部２５０６において繰り返すか否かの判定を行なう為に、初期値として変数Ｉに１を代入する。ステップ２２０２として、２倍算演算部２５０４により、点Ｐの２倍点２Ｐを計算する。ステップ２２０３として、スカラー倍計算装置２５０１に入力された点Ｐとステップ２２０２で求めた点２Ｐを、点格納部２５０２に点の組（Ｐ，２Ｐ）として格納する。

【００８１】

ステップ２２０４として、繰り返し判定部２５０６により、変数Ｉとスカラー値のビット長とが一致するかどうかを判定し、一致すればステップ２２１３へ行く。一致しなければステップ２２０５へ行く。ステップ２２０５として、変数Ｉを１増加させる。ステップ２２０６として、ビット値判定部２５０５により、スカラー値のＩ番目のビットの値が０であるか１であるかを判定する。そのビットの値が０であればステップ２４０１へ行く。そのビットの値が１であればステップ２３０１へ行く。

【００８２】

ステップ２３０１として、演算ランダム化部２５０９により、加算及び２倍算の計算順序をランダム化する。加算、２倍算の順序で計算を実行する場合はステップ２３０５へ行く。２倍算、加算の順序で計算を実行する場合はステップ２３０２へ行く。

【００８３】

ステップ２３０２として、２倍算演算部２５０４により、点格納部２５０２に格納されている点の組（ｍＰ，（ｍ＋１）Ｐ）から点（ｍ＋１）Ｐの２倍算２（（ｍ＋１）Ｐ）を行ない、点（２ｍ＋２）Ｐを計算する。その後ステップ２３０３へ行く。ステップ２３０３として、加算演算部２５０３により、点格納部２５０２に格納されている点の組（ｍＰ，（ｍ＋１）Ｐ）から点ｍＰと点（ｍ＋１）Ｐの加算ｍＰ＋（ｍ＋１）Ｐを行ない、点（２ｍ＋１）Ｐを計算する。その後ステップ２３０４へ行く。

【００８４】

ステップ２３０５として、加算演算部２５０３により、点格納部２５０２に格納されている点の組（ｍＰ，（ｍ＋１）Ｐ）から点ｍＰと点（ｍ＋１）Ｐの加算ｍＰ＋（ｍ＋１）Ｐを行ない、点（２ｍ＋１）Ｐを計算する。その後ステップ２３０６へ行く。ステップ２３０６として、２倍算演算部２５０４により、点格納部２５０２に格納されている点の組（ｍＰ，（ｍ＋１）Ｐ）から点（ｍ＋１）Ｐの２倍算２（（ｍ＋１）Ｐ）を行ない、点（２ｍ＋２）Ｐを計算する。その後ステップ２３０４へ行く。

【００８５】

ステップ２３０４として、ステップ２３０３乃至はステップ２３０５で求めた点（２ｍ＋１）Ｐとステップ２３０２乃至はステップ２３０６で求めた点（２ｍ＋２）Ｐを点格納部２５０２に点の組（（２ｍ＋１）Ｐ，（２ｍ＋２）Ｐ）として、点の組（ｍＰ，（ｍ＋１）Ｐ）の代わりに格納する。その後ステップ２２０４へ戻る。

【００８６】

ステップ２４０１として、演算ランダム化部２５０９により、加算及び２倍算